

《计算机网络》课程设计 ——DNS中继服务器的实现

程莉

chengli@bupt.edu.cn

2020年5月



北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

课程安排

■ 时间安排

- 课堂讲解1次
- QQ群（1048262028）讨论及答疑
- 其他时间独立进行编程实践

■ 实验环境

- 操作系统 Windows, Linux, ...
- 编程语言 C

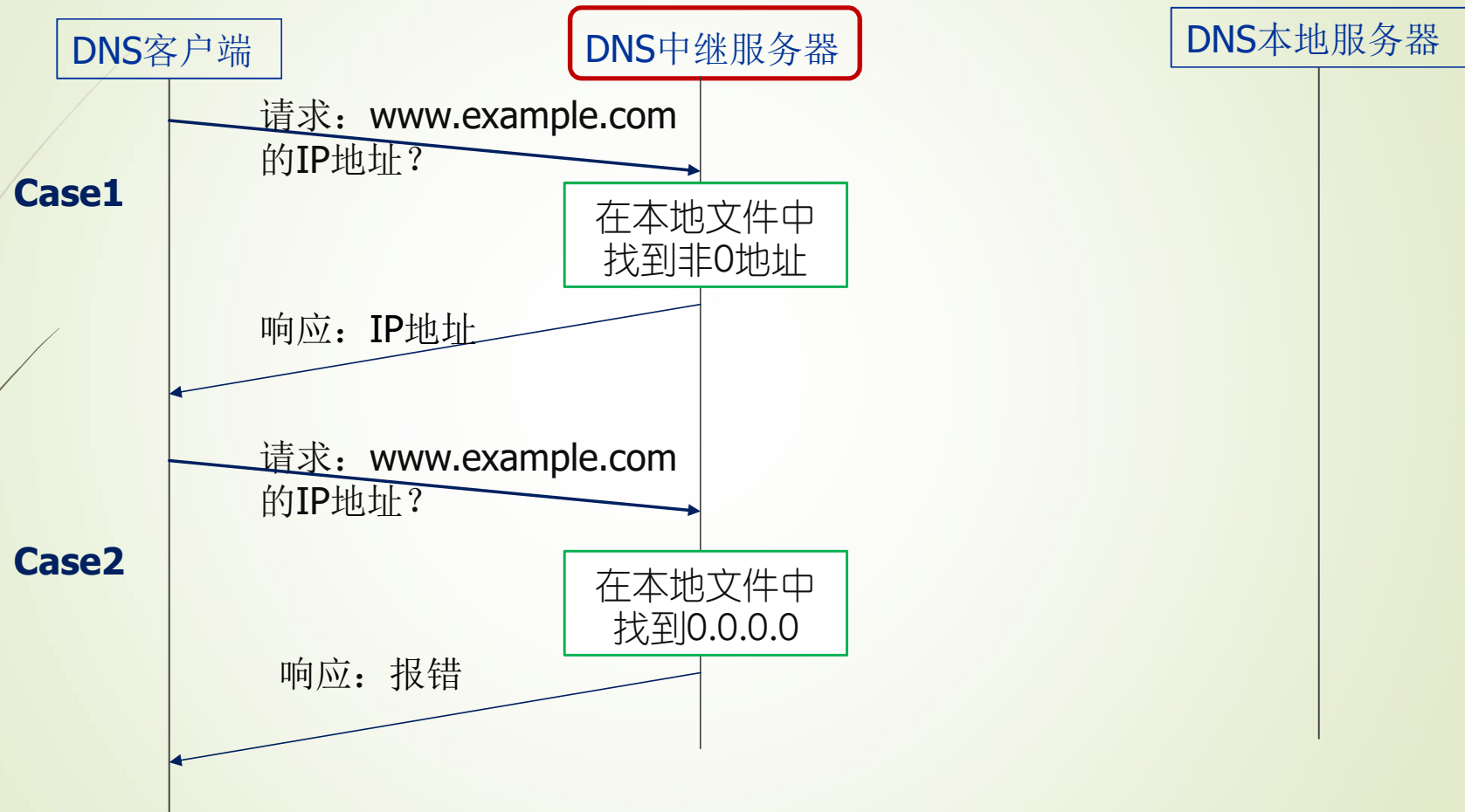
■ 分组（1-3人）

- 小组全体成员均需掌握所提交的程序，能经得起质疑

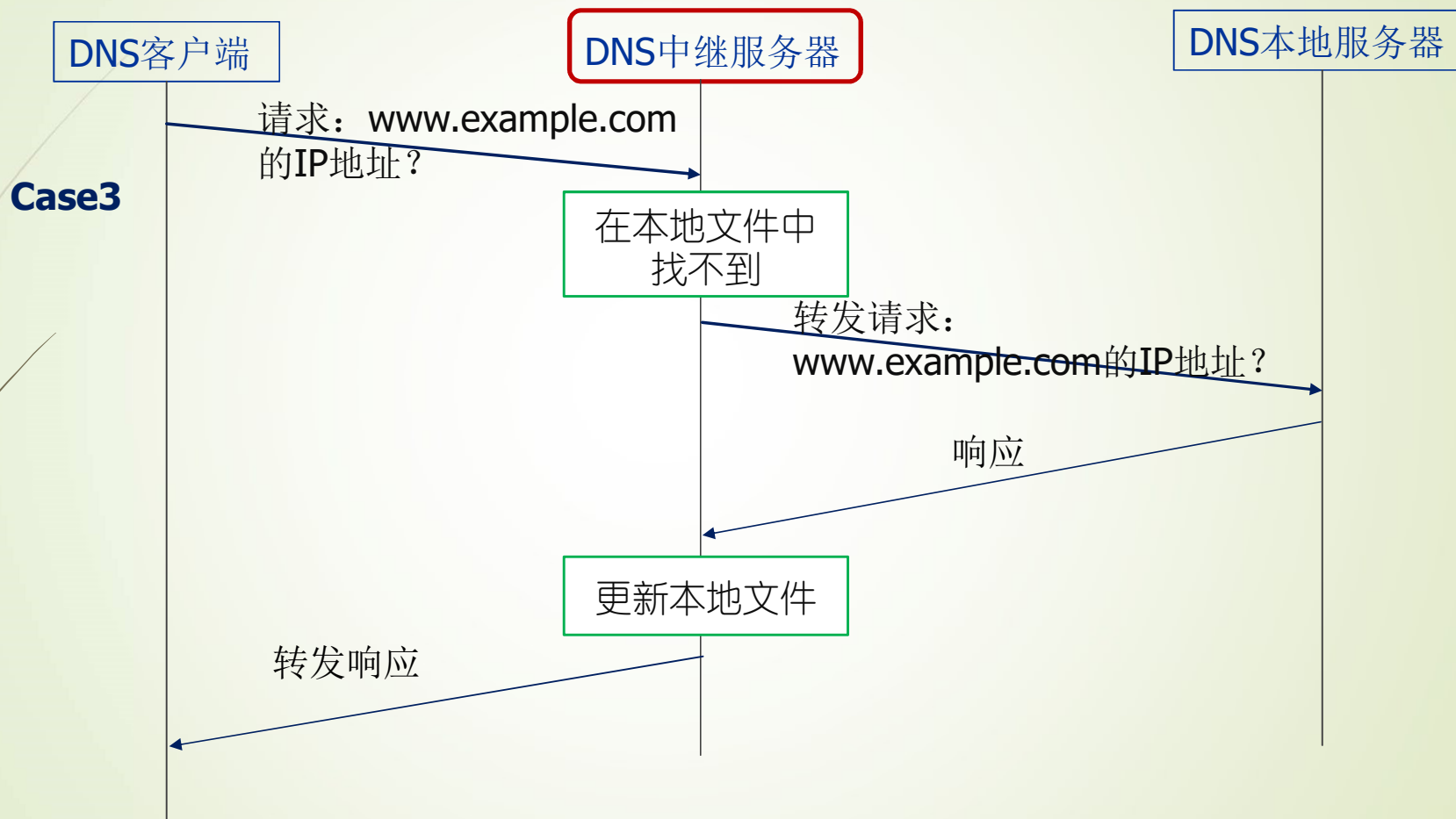
课程设计题目： DNS中继服务器的实现

- 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：
 - 检索结果为普通IP地址，则向客户返回这个地址（即DNS服务器功能）
 - 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）
 - 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）
 - 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

DNS中继服务器的基本功能（1）：DNS服务器



DNS中继服务器的基本功能（2）：DNS中继



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
- 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

- 验收方式：现场验收，时间：待定
 - 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；教师可能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

《计算机网络课程设计》

DNS: Domain Name System(域名系统)

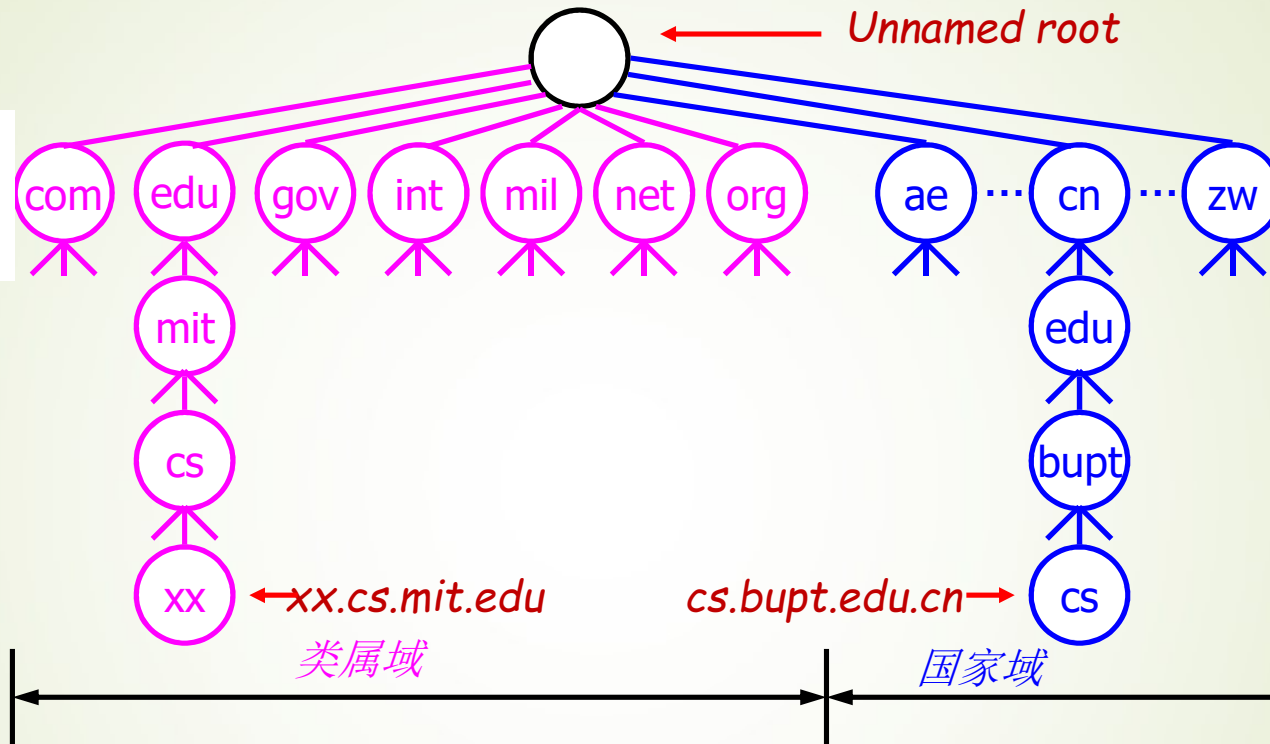
- ➡ 域名：用户友好的名字，用于标识因特网上的主机
 - 例如：`www.bupt.edu.cn`
- ➡ DNS的功能：域名管理、将域名转换为对应的IP地址
- ➡ 为其他因特网应用提供支持
- ➡ 采用Client-Server模式
- ➡ 传输层主要使用UDP
- ➡ 特点
 - 层次化的命名空间：主机的域名是分级命名的
 - 采用分布式数据库存储和管理域名

层次化的命名空间

11

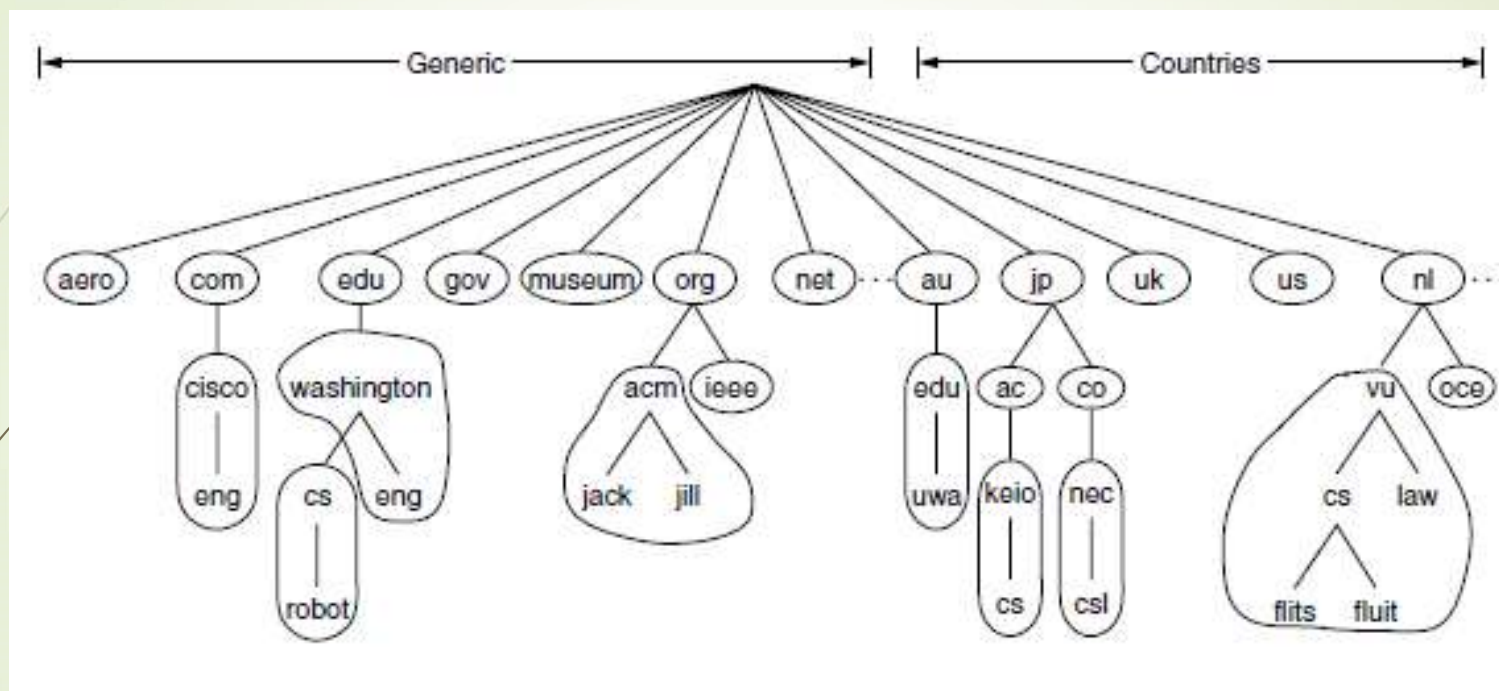
Top level domains
(顶级域名)

二级域



- 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

☒ : 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 (Resource Records)

- 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

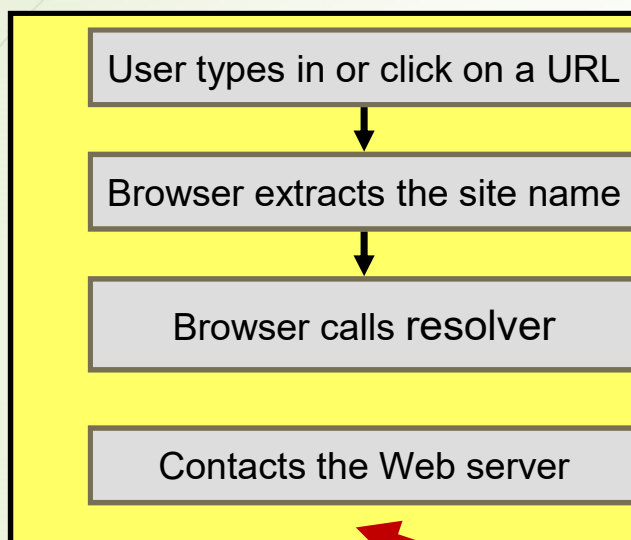
rowboat        IN      A       130.37.56.201
               IN      MX      1 rowboat
               IN      MX      2 zephyr

little-sister  IN      A       130.37.62.23

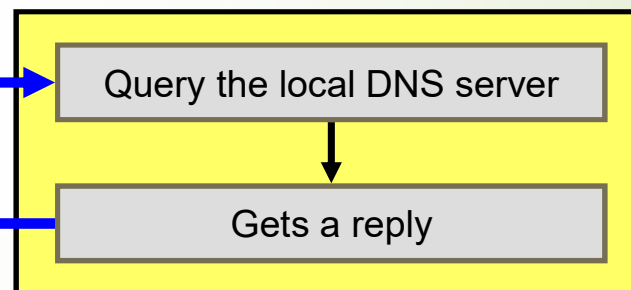
laserjet       IN      A       192.31.231.216
  
```

DNS客户端: resolver(解析器)

Browser(浏览器)



Resolver

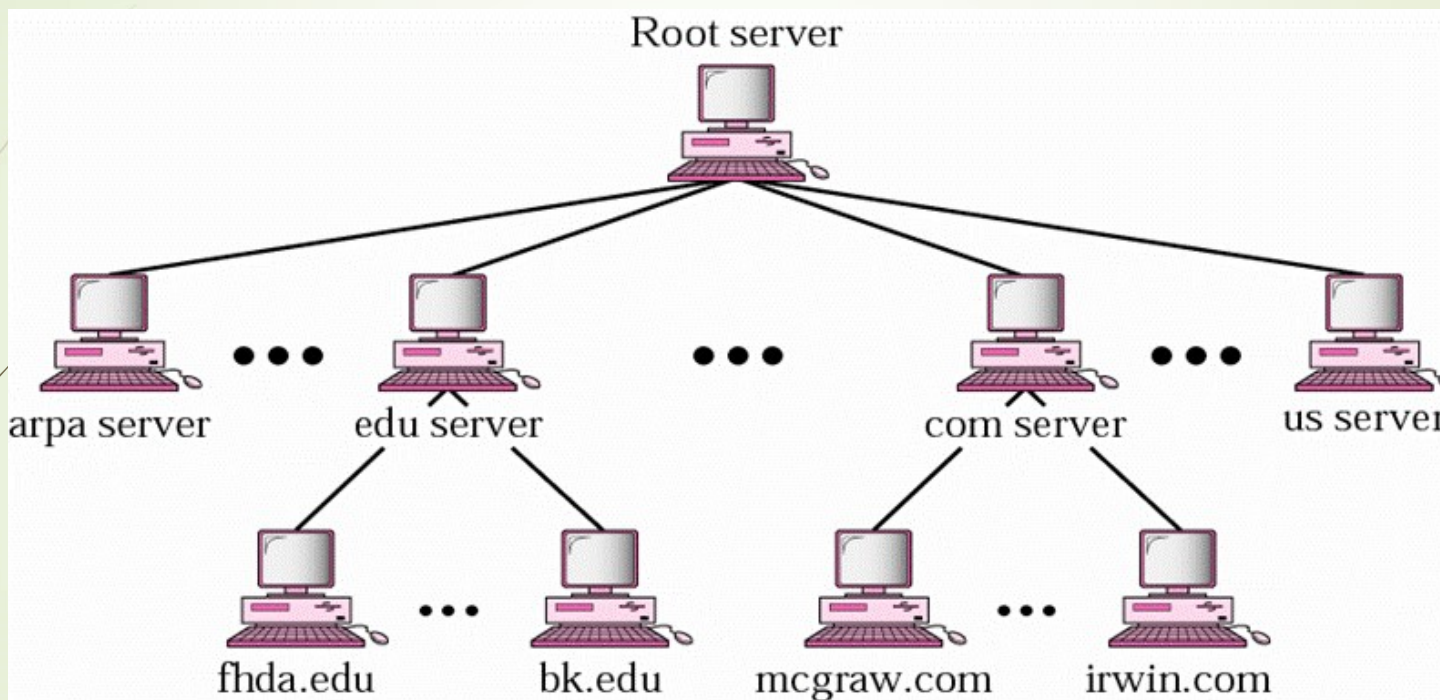


Web server

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名字：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

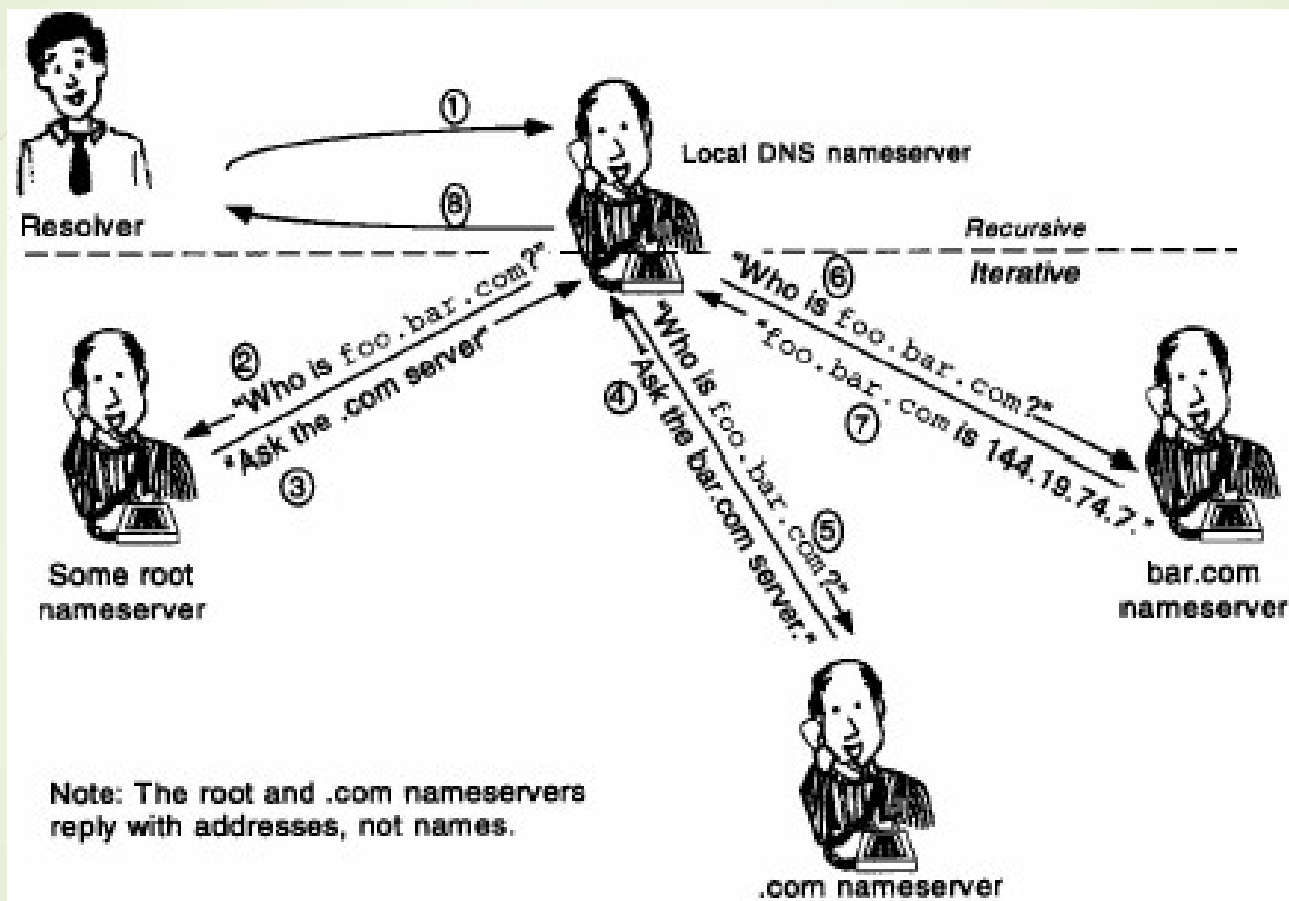
名字服务器的层次结构



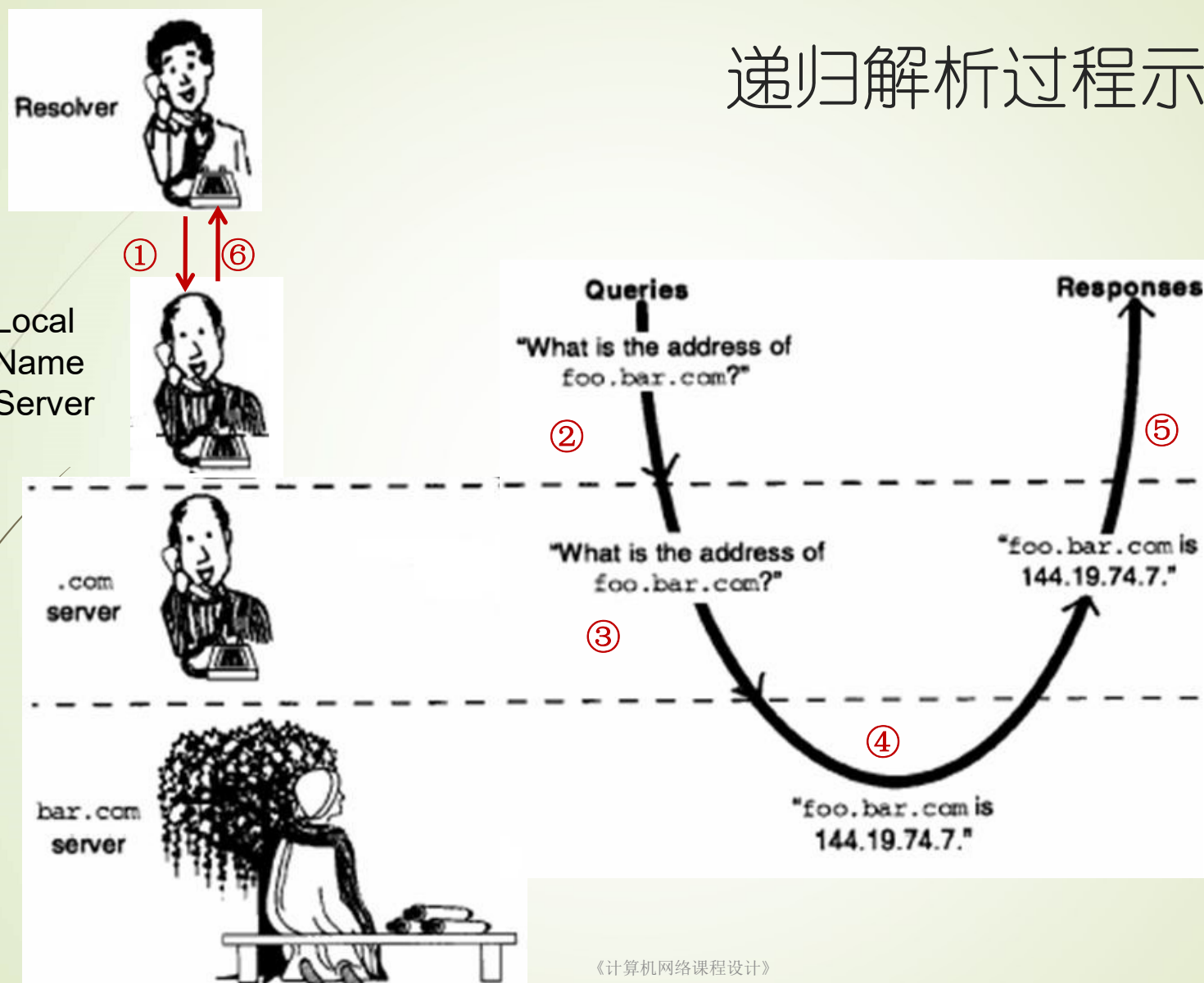
DNS域名解析

- ➡ 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:\Users\Administrator>nslookup www.bupt.edu.cn
```

```
服务器:  bogon
```

```
Address:  192.168.0.100
```

```
非权威应答:
```

```
名称:      vn.bupt.edu.cn
```

```
Addresses: 2001:da8:215:4038::161
```

```
           211.68.69.240
```

```
Aliases:   www.bupt.edu.cn
```

```
C:\Users\Administrator>nslookup -query=MX bupt.edu.cn
```

```
服务器:  bogon
```

```
Address:  192.168.0.100
```

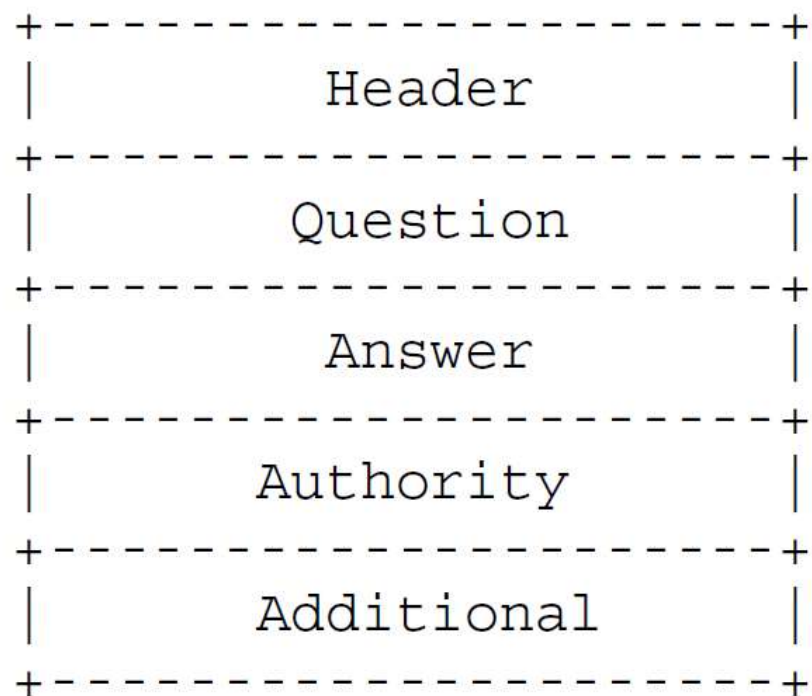
```
非权威应答:
```

```
bupt.edu.cn      MX preference = 10, mail exchanger = mxbiz2.qq.com
```

```
bupt.edu.cn      MX preference = 5, mail exchanger = mxbiz1.qq.com
```

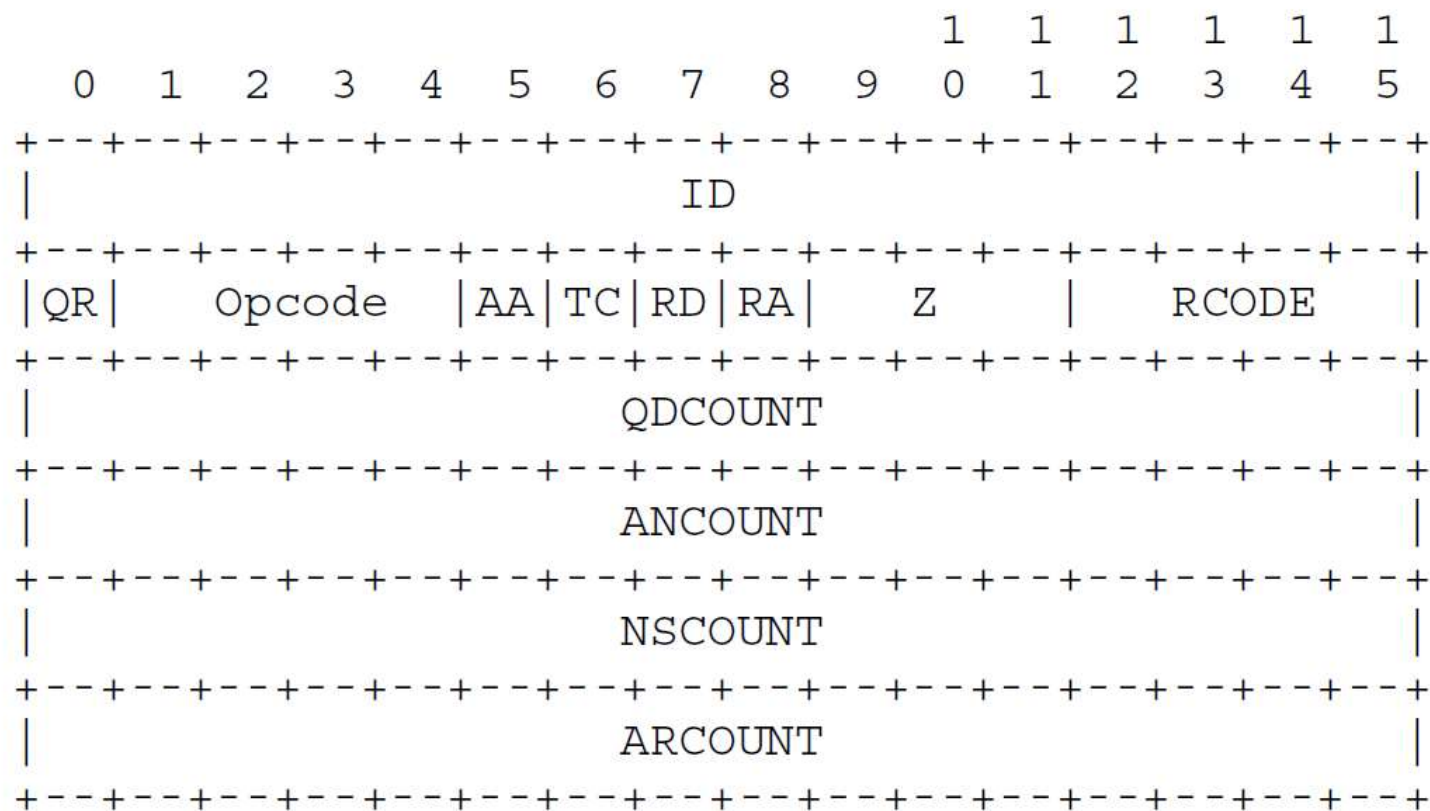
DNS的报文构成(RFC1035 4.1)

- 由5部分构成，除报头（Header）外其余四部分为可变长度



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)



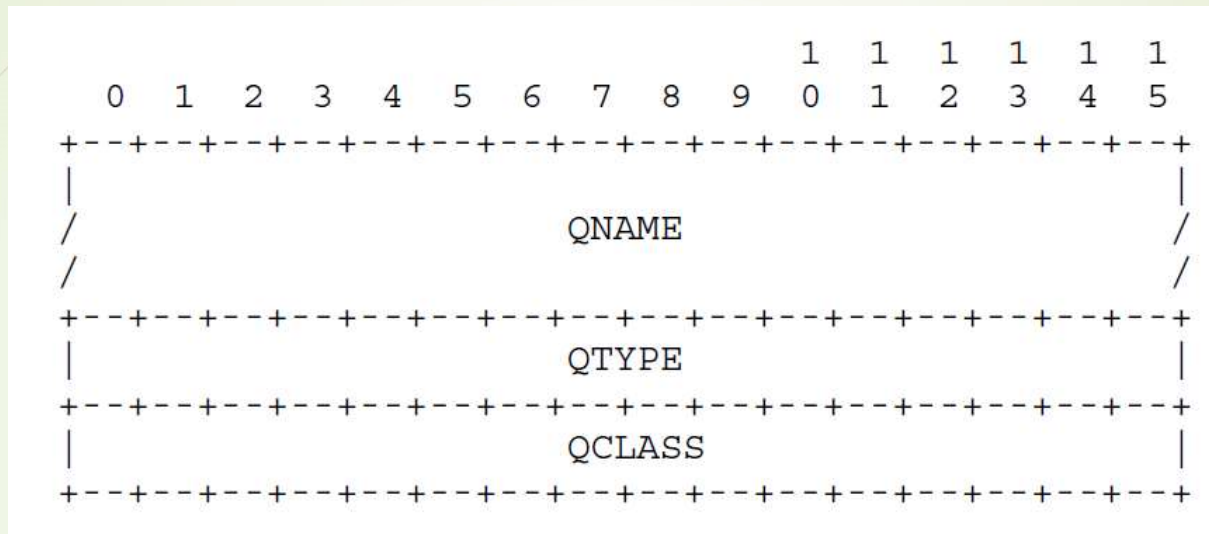
报头字段(1)

- 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)
 - ◆ 查询报文中设置, 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)

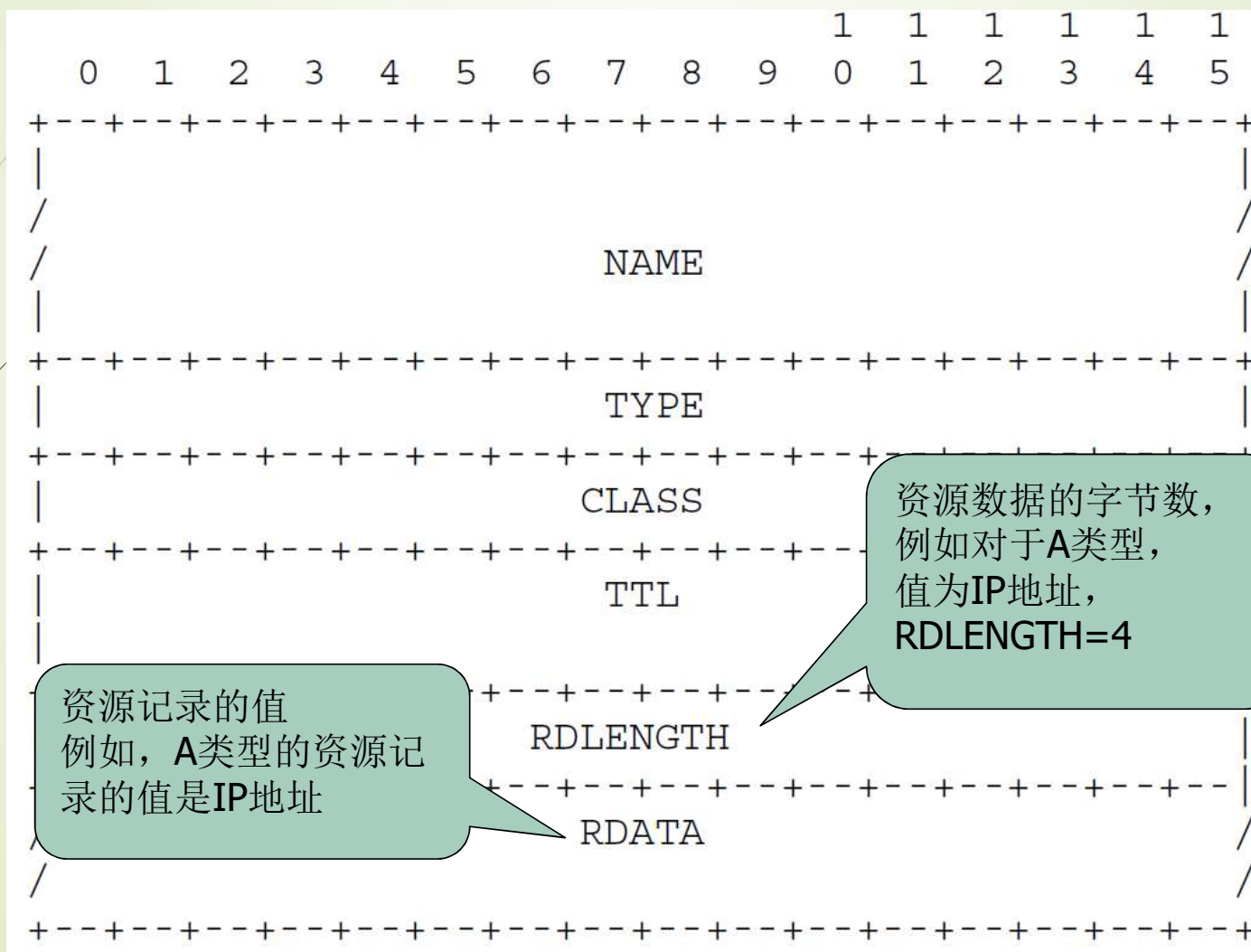
- Z: 必须为0, 保留字段
- RCODE: 响应码(Response coded), 仅用于响应报文
 - ◆ 值为0(没有差错)
 - ◆ 值为3表示名字差错。从权威名字服务器返回, 表示在查询中指定域名不存在
- QDCOUNT
 - ◆ question section的问题个数
- ANCOUNT
 - ◆ answer section的RR个数
- NSCOUNT
 - ◆ authority records section的RR个数
- ARCOUNT
 - ◆ additional records section的RR个数

Question Section的格式 (RFC1035 4.1.2)



- QNAME: 域名, 例如 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”

资源记录的格式(RFC1035 4.1.3)



报文示例 (RFC1034 6.2.1)

QNAME=SRI-NIC. ARPA, QTYPE=A

Header	OPCODE=QUERY, RESPONSE, AA
Question	QNAME=SRI-NIC. ARPA., QCLASS=IN, QTYPE=A
Answer	SRI-NIC. ARPA. 86400 IN A 26. 0. 0. 73 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

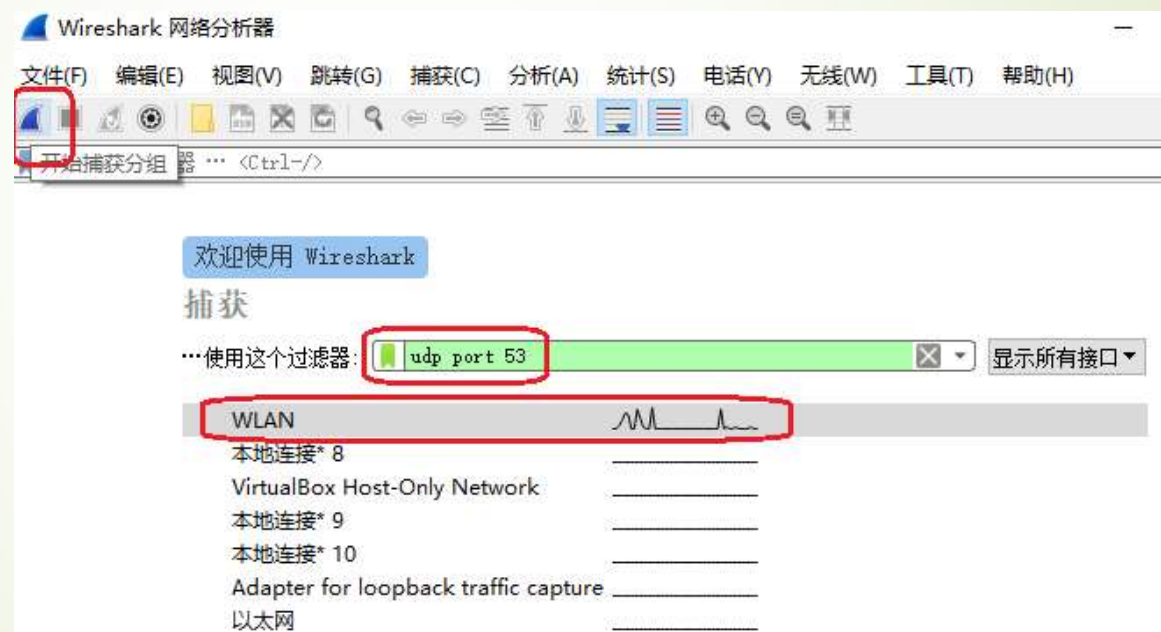
- Socket编程(自己查找相应文献)
- RFC1035协议文本
- http://en.wikipedia.org/wiki/Domain_Name_System
- 软件工具WireShark

关于Wireshark

- 免费的网络协议分析软件
- <http://www.wireshark.org/>
- 原名Ethereal，2006更名为Wireshark
- 能够捕获网络中传输的数据包，显示包中各字段的值及其含义
- 广泛用于网络协议的学习、开发、分析及查错

Wireshark的设置

- 设置接口：活跃的网卡
- 捕获过滤器：**udp port 53**



Wireshark捕获到的DNS报文示例：请求报文

- 触发DNS通信：在命令行窗口输入：nslookup www.bupt.edu.cn

报文概要

No.	Time	Source	Destination	Protocol	Length	Info
7	21.239060	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x0002 A www.bupt.edu.cn
8	21.244855	192.168.0.100	192.168.0.107	DNS	91	Standard query response 0x0002 A www.bup
9	21.245313	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x0003 AAAA www.bupt.edu.
10	21.249985	192.168.0.100	192.168.0.107	DNS	120	Standard query response 0x0003 AAAA www.
11	21.276668	192.168.0.107	192.168.0.100	DNS	86	Standard query 0x3ef1 A 100.0.168.192.in
12	21.283298	192.168.0.100	192.168.0.107	DNS	136	Standard query response 0x3ef1 A 100.0.1
13	21.386154	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x3c5b A www.bupt.edu.cn
14	21.396751	192.168.0.100	192.168.0.107	DNS	91	Standard query response 0x3c5b A www.bup

> Ethernet II, Src: IntelCor_a7:ec:d4 (cc:2f:71:a7:ec:d4), Dst: D-LinkIn_e2:f9:24 (78:54:2e:e2:f9:24)
> Internet Protocol Version 4, Src: 192.168.0.107, Dst: 192.168.0.100
> User Datagram Protocol, Src Port: 60571, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries
> www.bupt.edu.cn: type A, class IN

报文详细内容

Wireshark捕获到的DNS报文示例：响应报文

No.	Time	Source	Destination	Protocol	Length	Info
7	21.239060	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x0002 A www.bupt.edu.cn
8	21.244855	192.168.0.100	192.168.0.107	DNS	91	Standard query response 0x0002 A www.bupt.edu.cn A 211.68.69...
9	21.245313	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x0003 AAAA www.bupt.edu.cn
10	21.249985	192.168.0.100	192.168.0.107	DNS	120	Standard query response 0x0003 AAAA www.bupt.edu.cn CNAME vn...
11	21.276668	192.168.0.107	192.168.0.100	DNS	86	Standard query 0x3ef1 A 100.0.168.192.in-addr.arpa
12	21.283298	192.168.0.100	192.168.0.107	DNS	136	Standard query response 0x3ef1 A 100.0.168.192.in-addr.arpa S...
13	21.386154	192.168.0.107	192.168.0.100	DNS	75	Standard query 0x3c5b A www.bupt.edu.cn
14	21.396751	192.168.0.100	192.168.0.107	DNS	91	Standard query response 0x3c5b A www.bupt.edu.cn A 211.68.69...

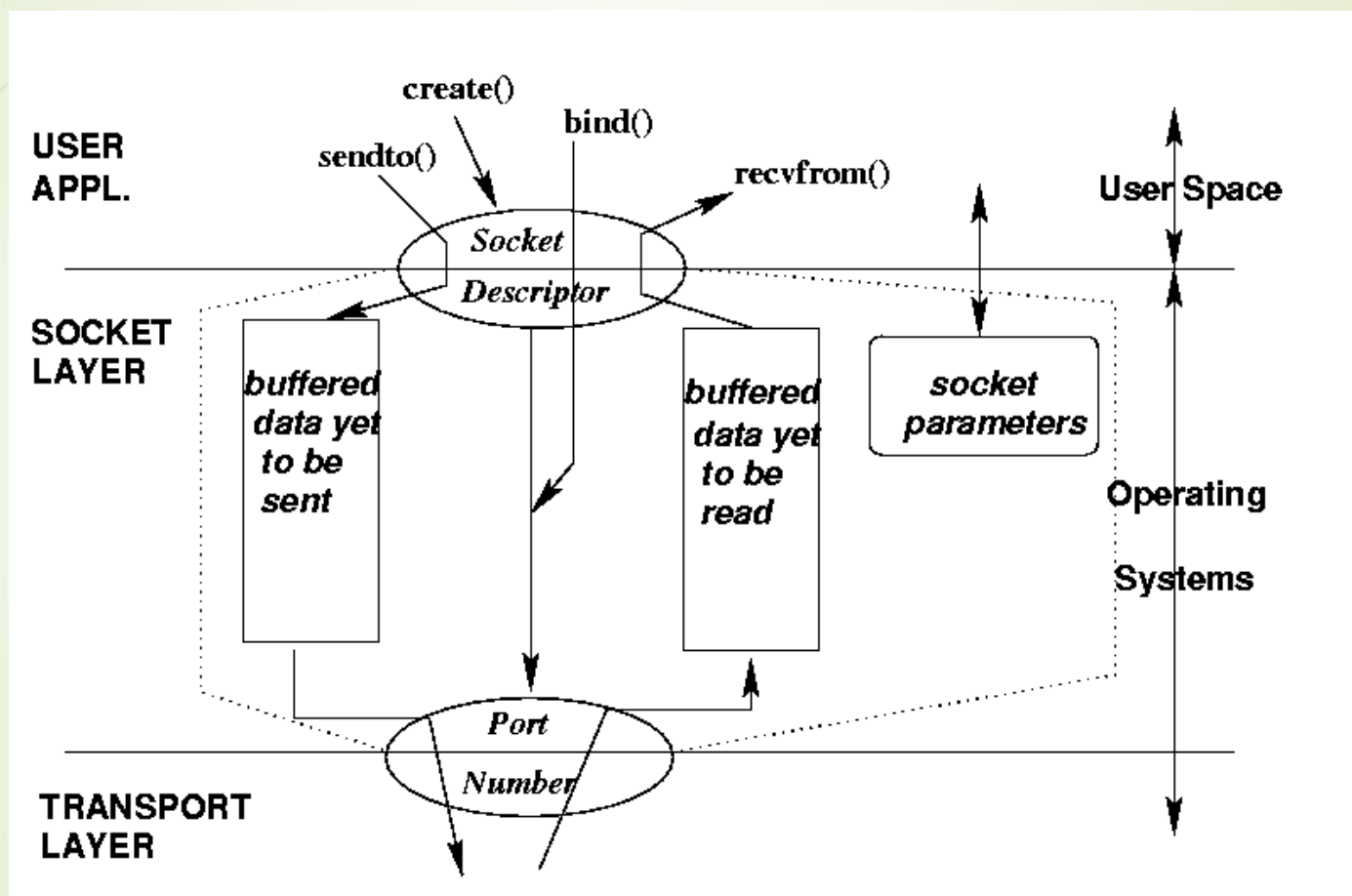
```

> Frame 8: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{4EC921DB-E113-433B-AD18-433EFDA35CF4}, id 0
> Ethernet II, Src: D-LinkIn_e2:f9:24 (78:54:2e:e2:f9:24), Dst: IntelCor_a7:ec:d4 (cc:2f:71:a7:ec:d4)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.107
> User Datagram Protocol, Src Port: 53, Dst Port: 60571
v Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.bupt.edu.cn: type A, class IN
  v Answers
    > www.bupt.edu.cn: type A, class IN, addr 211.68.69.240

```

程序的设计和运行

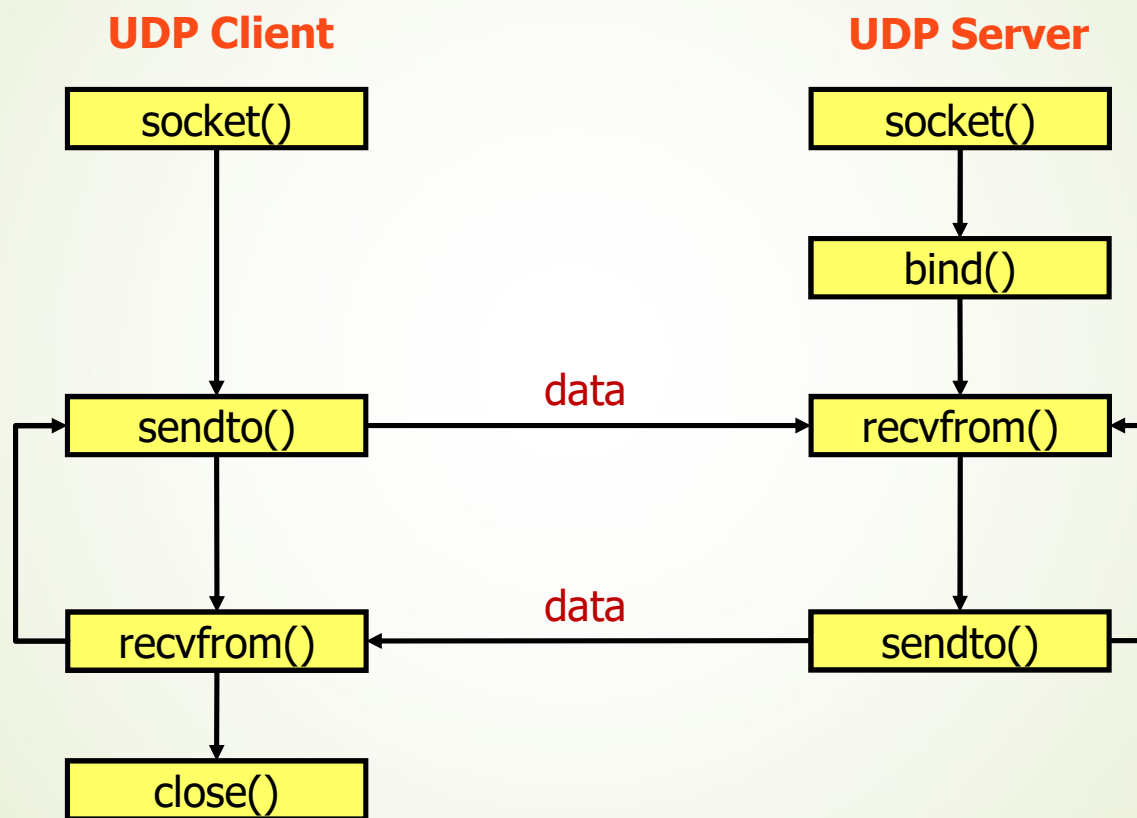
SOCKET的概念模型



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



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 Endian
- 网络字节序 (NBO)
 - 高阶字节先发送/接收—— Big Endian
- 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（1）

■ 运行步骤

1. 使用ipconfig /all,记下当前DNS服务器的IP地址
■ 例如为10.3.9.4
2. 使用本机的网络配置界面，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10.3.9.4)
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

Windows系统下DNS中继服务器的运行（1）

➤ 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

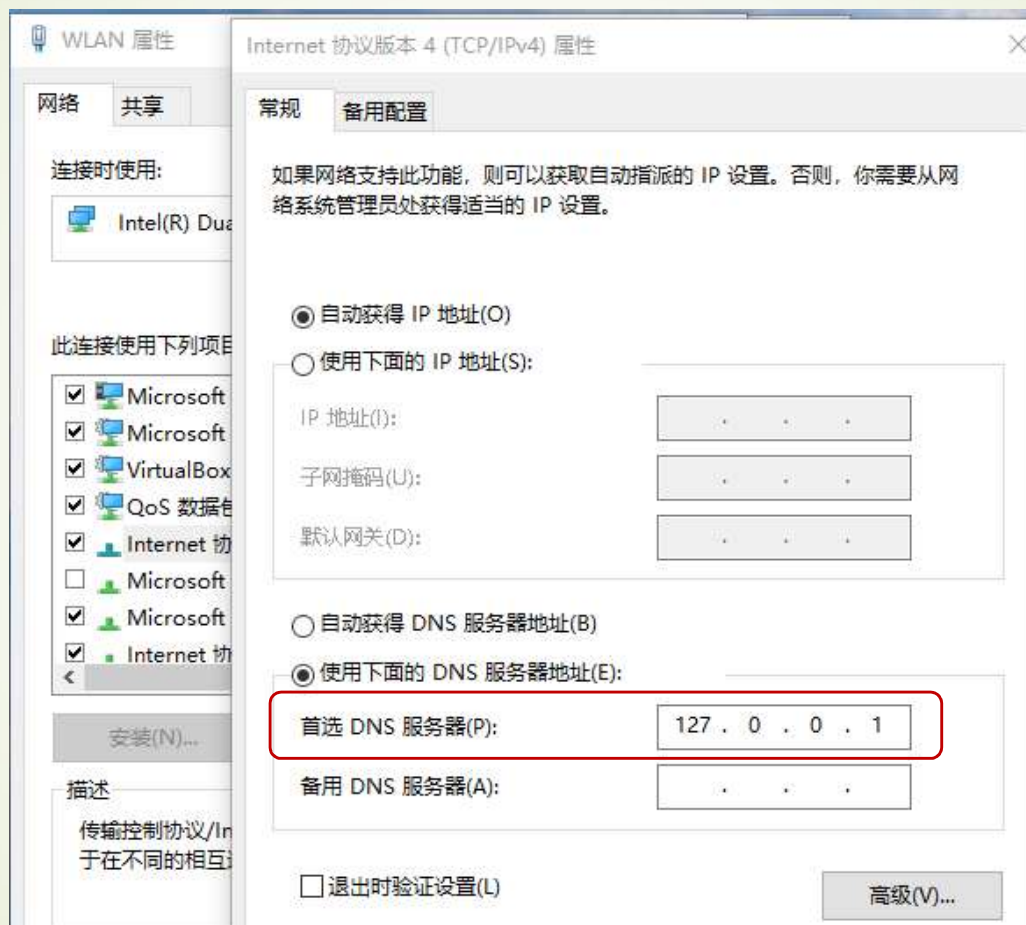
◆ Ipconfig /displaydns

➤ 查看当前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



程序必须要考虑的两个问题

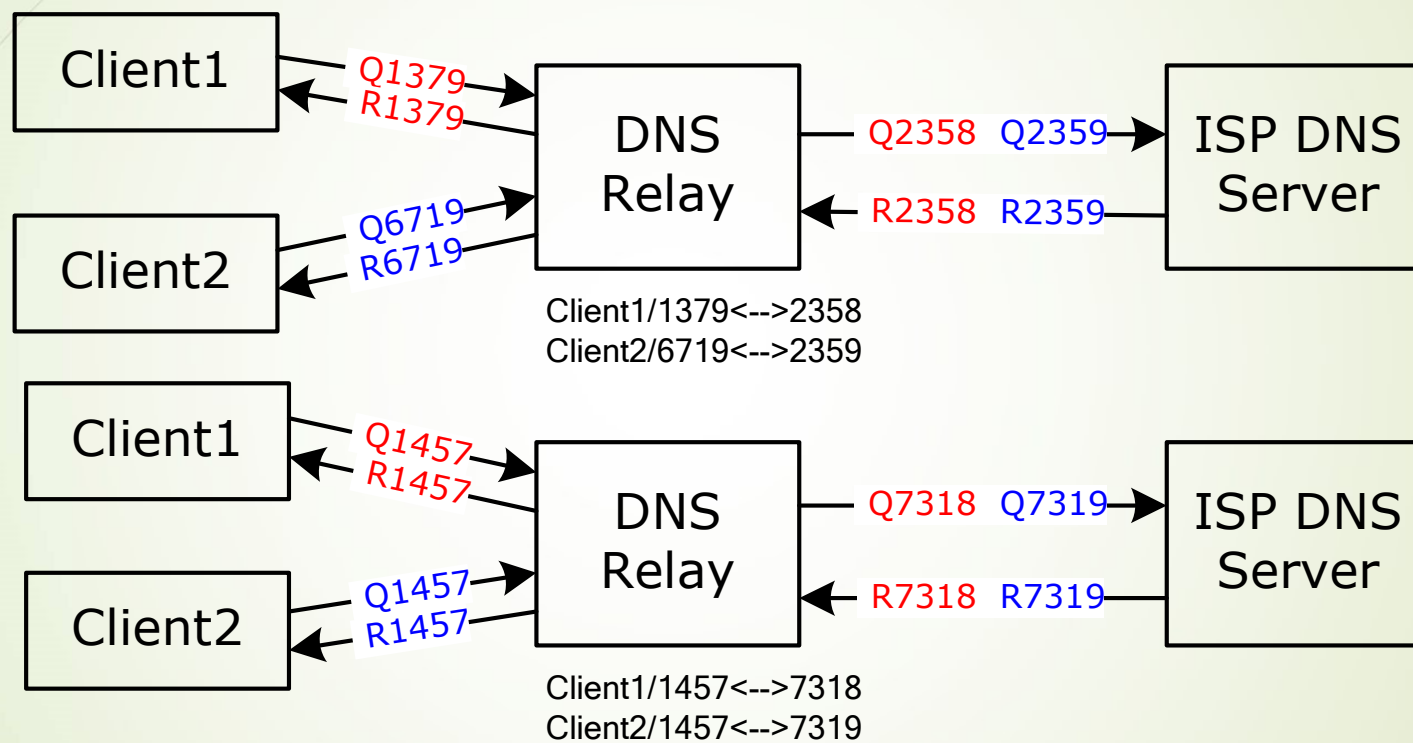
➡ 多客户端并发

- 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)

可扩展功能

- 实现AAAA类型的资源记录查询功能
- 实现MX类型、CNAME类型的资源记录查询功能
- 实现资源记录的缓存及从缓存中查询功能
-

参考实现

命令行语法示例

47

- `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)

参考程序运行示例

```
D:\dns-test>dnsrelay -d 192.168.0.100
DNSRELAY, Version 1.30, Build: Feb 22 2011 10:08:17
Usage: dnsrelay [-d | -dd] [<dns-server>] [<db-file>]

Name server 192.168.0.100:53.
Debug level 1.
Bind UDP port 53 ...OK!
Try to load table "dnsrelay.txt" ... OK
909 names, occupy 23511 bytes memory
 0: 2020-05-05 19:15:30 Client 127.0.0.1 dr-ime.baidu.com
 1: 2020-05-05 19:15:30 Client 127.0.0.1 dr-ime.baidu.com
 2: 2020-05-05 19:15:38 Client 127.0.0.1 olime.baidu.com
 3: 2020-05-05 19:15:58 Client 127.0.0.1 1.0.0.127.in-addr.arpa, TYPE 12, CLASS 1
 4: 2020-05-05 19:15:59 Client 127.0.0.1 1.0.0.127.in-addr.arpa
 5: 2020-05-05 19:15:59 Client 127.0.0.1 www.bupt.edu.cn
 6: 2020-05-05 19:15:59 Client 127.0.0.1 www.bupt.edu.cn, TYPE 28, CLASS 1
 7: 2020-05-05 19:15:59 Client 127.0.0.1 1.0.0.127.in-addr.arpa
 8: 2020-05-05 19:15:59 Client 127.0.0.1 1.0.0.127.in-addr.arpa
 9: 2020-05-05 19:16:00 Client 127.0.0.1 www.bupt.edu.cn
10: 2020-05-05 19:16:26 Client 127.0.0.1 tingmb.bding.com
11: 2020-05-05 19:16:28 Client 127.0.0.1 cpro.baidustatic.com
12: 2020-05-05 19:16:30 Client 127.0.0.1 dr-ime.baidu.com
13: 2020-05-05 19:16:40 Client 127.0.0.1 1.0.0.127.in-addr.arpa, TYPE 12, CLASS 1
14:* 2020-05-05 19:16:40 Client 127.0.0.1 555.265.com
15:* 2020-05-05 19:16:40 Client 127.0.0.1 555.265.com
16: 2020-05-05 19:16:40 Client 127.0.0.1 555.265.com, TYPE 28, CLASS 1
```


DNS客户端执行示例

```
C:\Users\Administrator>nslookup www.bupt.edu.cn
服务器: localhost
Address: 127.0.0.1
```

中继功能

```
非权威应答:
名称:      vn.bupt.edu.cn
Addresses: 2001:da8:215:4038::161
           211.68.69.240
Aliases:   www.bupt.edu.cn
```

```
C:\Users\Administrator>nslookup 555.265.com
服务器: localhost
Address: 127.0.0.1
```

查到0.0.0.0

```
*** localhost 找不到 555.265.com: Non-existent domain
```

```
C:\Users\Administrator>nslookup www.bupt.com.cn
服务器: localhost
Address: 127.0.0.1
```

本地文件查到

```
名称:      www.bupt.com.cn
Address: 60.222.224.141
```