

第2章 应用层

SMTP、FTP和DNS协议

任课老师：周军海

Email:rj_zjh@hnu.edu.cn

2.3 因特网中的电子邮件

电子邮件快速、多方接收，包含附件、超链接、图像、声音、视频等等。

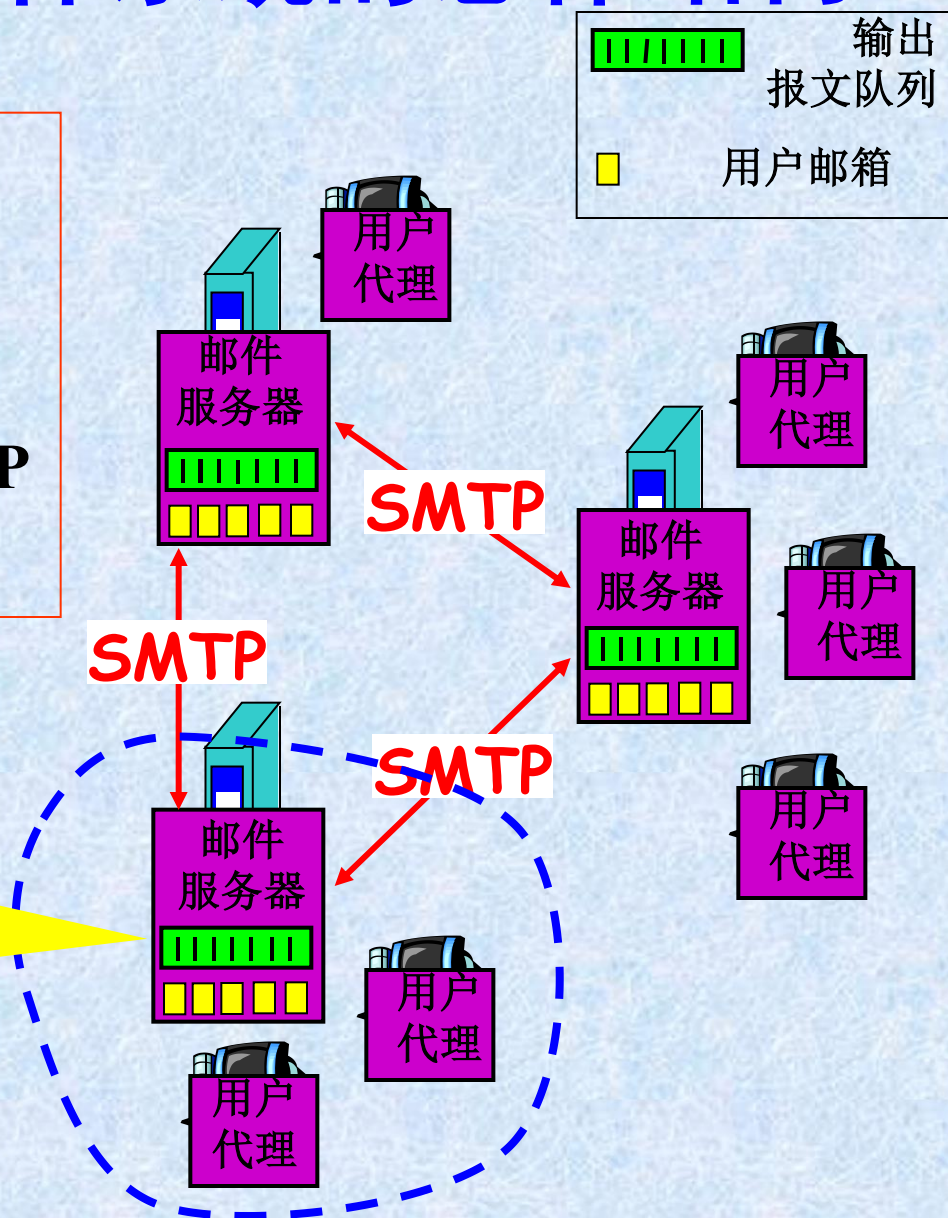
本节讨论电子邮件的核心，即应用层协议。

因特网电子邮件系统的总体结构

三部分：

- ✓ 用户代理
- ✓ 邮件服务器
- ✓ 简单邮件传输协议SMTP

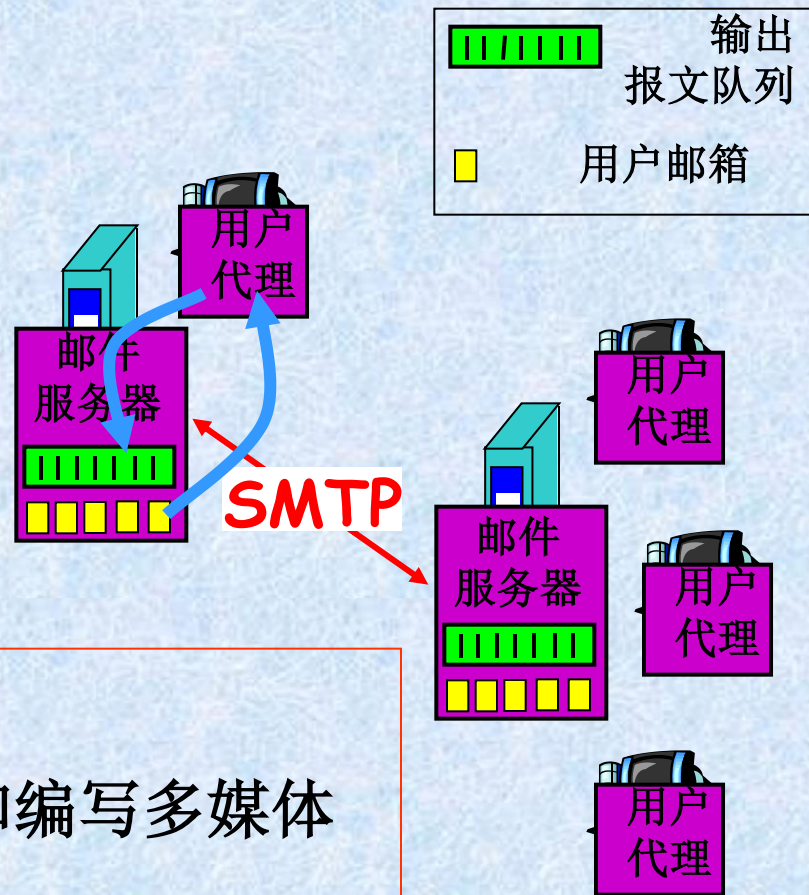
电子邮件地址
用户邮箱名@主机名



1、用户代理(user agent)

邮件阅读器。允许用户阅读、回复、发送、保存和撰写报文。

- ✓ 当用户完成邮件撰写时，**邮件代理**向其**邮件服务器**发送**邮件**，并存放在发送队列中。
- ✓ 当用户想读取一条报文时，**邮件代理**从其**邮件服务器的邮箱**中获取该报文。



□ 种类:

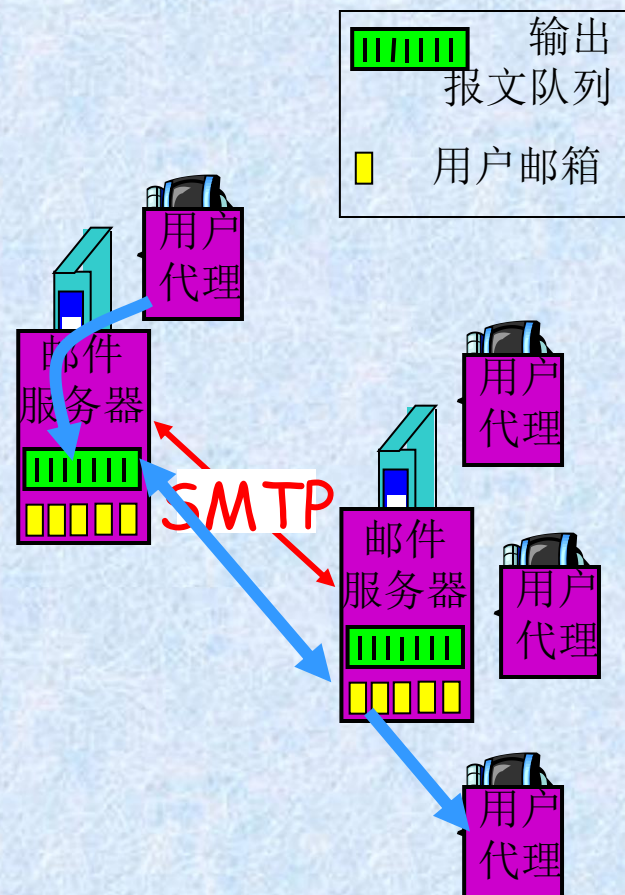
- ✓ **GUI (图形用户接口)**: 阅读和编写多媒体邮件。如**Outlook**、**Foxmail**等。

2、邮件服务器(mail server)

- ✓ **邮箱**：发送给用户的报文。
- ✓ **报文队列**：用户要发出的邮件报文。

□ 邮件发送主要过程：

- ✓ 邮件**保存**到发送方报文队列
- ✓ 通过**SMTP协议转发**到接收方邮件服务器，保存到相应邮箱中
 - 若投递失败，发送方将其保存在一个报文队列中，以后每30分钟发送一次，若几天后仍未成功，将该报文删除，并通知发送方。
 - 用户访问自己邮箱时，邮件服务器对其身份进行验证(用户名和口令)。



3、简单邮件传送协议SMTP

从发送方的邮件服务器向接收方的邮件服务器发送邮件。

- ✓ 应用层协议。
- ✓ 使用TCP可靠数据传输服务。
- 包括两部分：
 - ✓ 客户端：在发送方邮件服务器上运行；
 - ✓ 服务器端：在接收方邮件服务器上运行。

每个邮件服务器上都有SMTP的客户端和服务端。

本节内容

2.3.1 SMTP

2.3.2 SMTP与HTTP比较

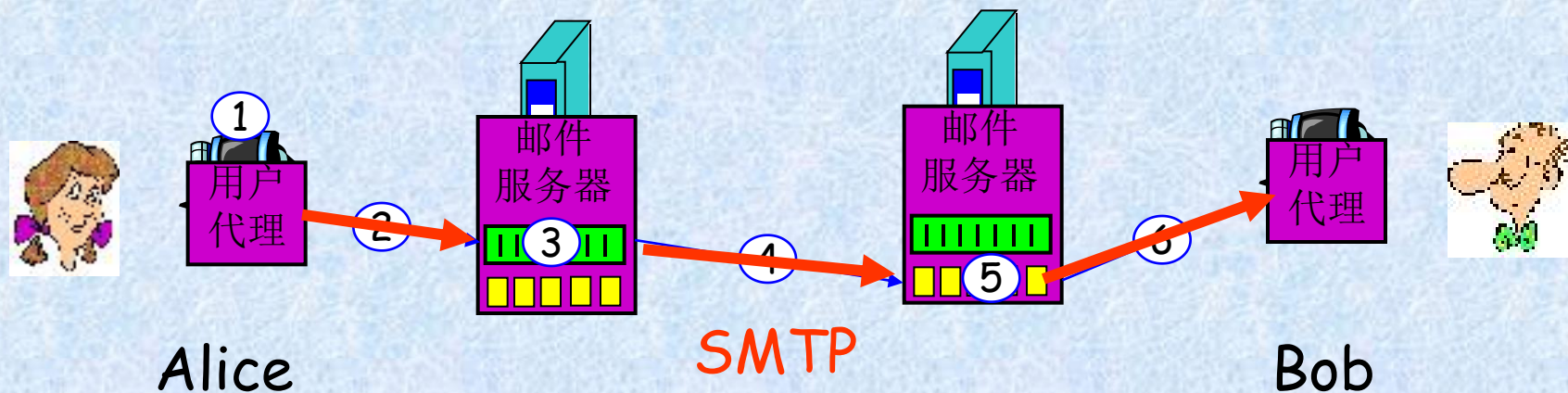
2.3.3 邮件报文格式和MIME

2.3.4 邮件访问协议

2.3.1 SMTP

把一封邮件从发送邮件服务器传送到接收邮件服务器的过程： 如Alice 向 Bob发送报文

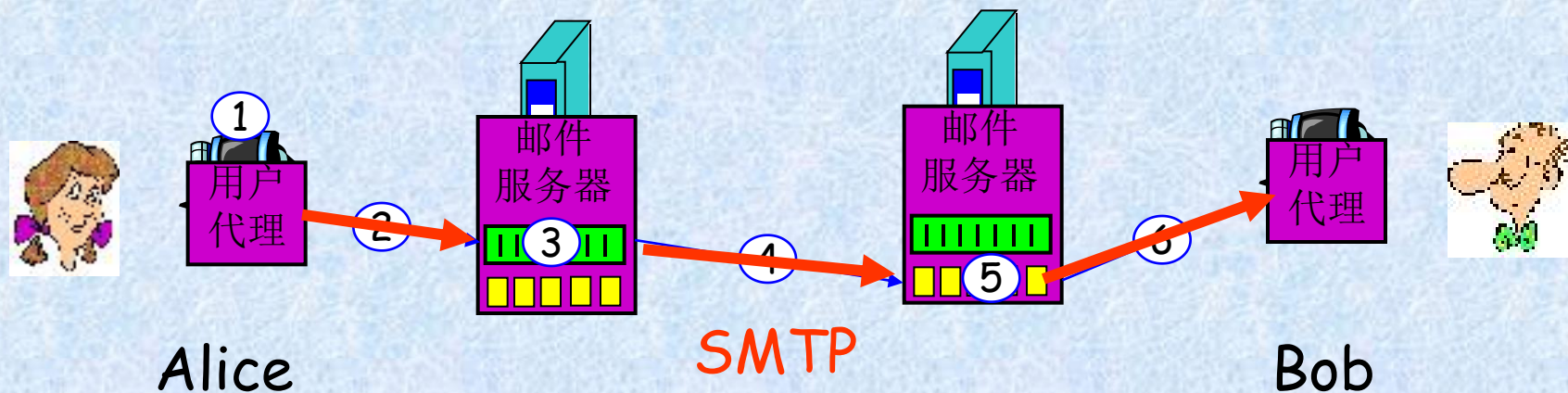
- 1) Alice启动邮件代理，提供接收方的邮件地址，撰写邮件
- 2) 用户代理把报文发给其邮件服务器，放在发送队列中
- 3) SMTP的客户机侧创建与Bob的邮件服务器的TCP连接
- 4) SMTP通过TCP连接发送报文
- 5) Bob的邮件服务器接收并将该报文放入Bob的邮箱
- 6) Bob调用其用户代理来读报文



2.3.1 SMTP

把一封邮件从发送邮件服务器传送到接收邮件服务器的过程： 如Alice 向 Bob发送报文

- 1) Alice启动邮件代理，提供接收方的邮件地址，撰写邮件
- 2) 用户代理把报文发给其邮件服务器，放在发送队列中
- 3) SMTP的客户机侧创建与Bob的邮件服务器的TCP连接
- 4) SMTP通过TCP连接发送报文
- 5) Bob的邮件服务器接收并将该报文放入Bob的邮箱
- 6) Bob调用其用户代理来读报文



说明

- 客户使用**TCP**来可靠传输邮件报文到服务器端口号25。
 - ✓ **建立TCP连接：**
 - ✓ **握手：** 指明收发双方的邮件地址
 - ✓ **邮件报文的传输**
 - ✓ **结束：** 关闭TCP连接

□ **SMTP不使用中间邮件服务器发送邮件，即TCP 连接是从发送方到接收方的直接相连。**

如果接收方的邮件服务器没有开机，该邮件仍保留在发送方邮件服务器上，并在以后进行再次传送。**邮件不会在某个中间邮件服务器停留。**

共同点

- ✓ 都用于从一台主机向另一台主机传送文件
 - ◆ **HTTP**用于从Web服务器向Web客户机(浏览器)传送文件 (对象);
 - ◆ **SMTP**用于从一个邮件服务器向另一个邮件服务器传送文件(电子邮件报文)。
- ✓ 持续: **HTTP**和**SMTP**都使用持续连接。

区别

□ HTTP是拉协议：用户使用HTTP从服务器拉取信息。其TCP连接是由想获取文件的机器发起。

SMTP是推协议：发送邮件服务器把文件推向接收邮件服务器，其TCP连接是由要发送文件的机器发起。

区别

❑ SMTP使用7位ASCII码格式:

对一些包含了**非7位ASCII**字符的报文或二进制数据(如图片、声音), **需要按照7位ASCII码进行编码, 再传送。**

在接收方需要解码还原为原有报文。

HTTP数据没有该限制。

❑ 对含有文本和图形 (或其他媒体类型) 的文档:

- ✓ HTTP把**每个对象封装**在它各自的HTTP响应报文中发送
- ✓ 电子邮件则把**所有报文对象**放在一个报文中。

邮件报文格式

- 首部行（收发人、主题）

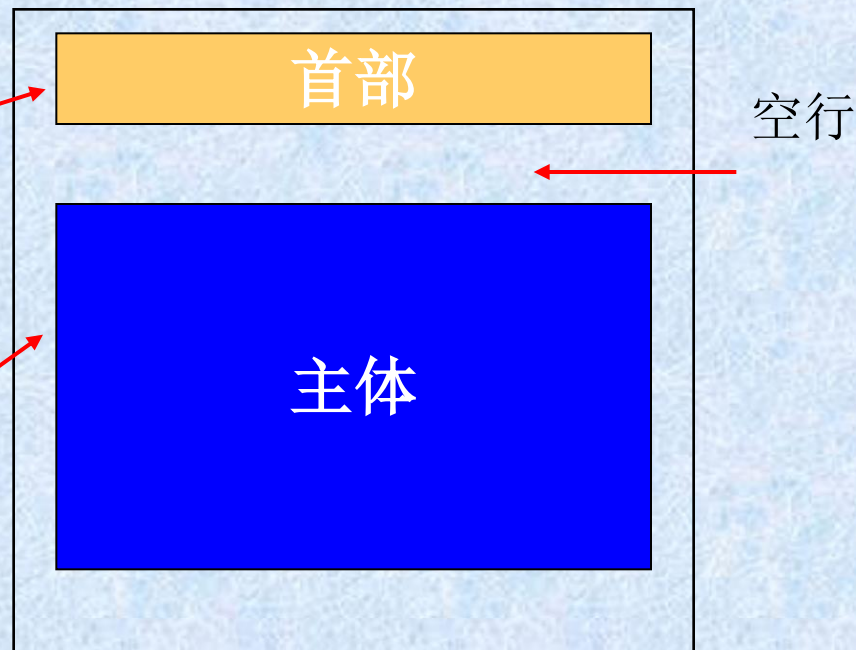
- To:

- From:

- Subject:

- 主体

- “报文”，均为ASCII
字符



MIME（多用途因特网邮件扩展）

- ✓ SMTP只传送7位的ASCII码。
- ✓ SMTP不能传送可执行文件或其他的二进制对象。

MIME：用于非ASCII数据传输。将非ASCII数据编码后传输，接收方再解码还原。

- ✓ 增加新的MIME邮件首部
- ✓ 采用某种编码

例：传输一个jpeg图形

jpeg格式的静止图像

base64编码：用于
二进制文件

MIME 版本

使用数据编码的方法

多媒体数据类型，
子类型，
声明参数

编码数据

```
From: Alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data .....
.....base64 encoded data
```


接收的报文

添加一个Received: 首部行

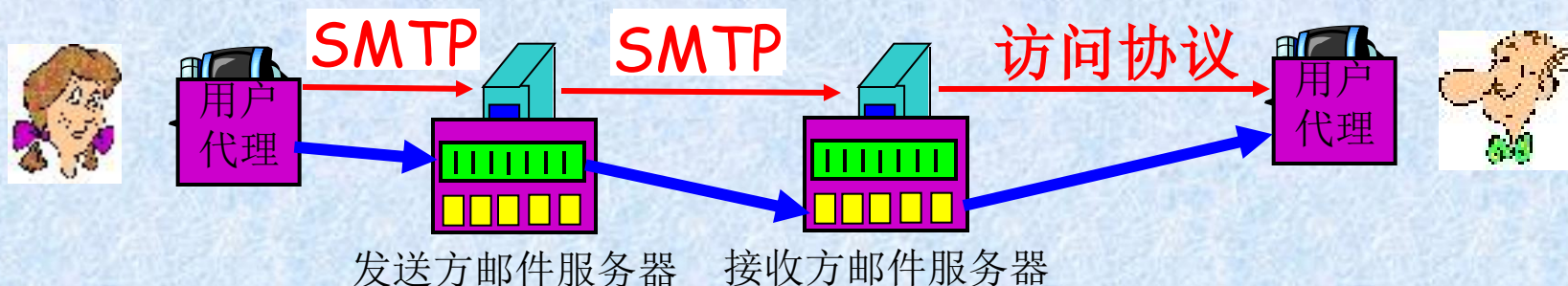
```
Received: from cress.fr by hamburger.edu;12  
oct 98 15:27:39 GMT
```

```
From: alice@crepes.fr  
To: bob@hamburger.edu  
Subject: Picture of yummy crepe.  
MIME-Version: 1.0  
Content-Transfer-Encoding: base64  
Content-Type: image/jpeg  
  
base64 encoded data .....  
.....  
.....base64 encoded data
```


2.3.4 邮件访问协议

- **发送方**：用户代理用**SMTP**将邮件推入其邮件服务器
→ 邮件服务器再用**SMTP**将邮件转发到接收方的邮件服务器
- **接收方**：通过其用户代理使用一个**邮件访问协议**（不是SMTP），从其邮件服务器上取回邮件。

取邮件是一个拉操作，而SMTP协议是一个推协议。



□ **邮件访问协议：**从服务器获取邮件。

□ **种类：**

POP3(第三版的邮局协议)

IMAP(因特网邮件访问协议)

HTTP(超文本传输协议)

1、POP3

简单、功能有限。

在用户代理打开了一个到邮件服务器(服务器)端口110上的TCP连接后，开始工作。

工作步骤（三阶段）：

- ✓ **特许阶段：** 用户代理发送用户名和口令获得下载邮件的特许。（**身份认证**）
- ✓ **事务处理阶段：** 用户代理取回报文，可对邮件进行某些操作。

如做删除标记、取消删除标记、获取统计信息等。

- ✓ **更新阶段：** 邮件服务器删除带有删除标记的报文，结束POP会话。

2、IMAP

- ❑ **POP3缺陷：** 用户读取邮件后，服务器不再保存。
- ❑ **IMAP：** 功能强
 - ✓ 在用户的PC机上运行IMAP客户程序，然后与ISP的邮件服务器上的IMAP服务器程序**建立TCP连接**。
 - ✓ 用户在自己的PC机上就可以操纵邮件服务器的邮箱，就像在本地操纵一样，是一个**联机协议**。
 - ✓ 未发出删除命令前，一直保存在邮件服务器
 - ✓ 实现起来复杂。

3、基于web的电子邮件

1995年12月Hotmail 引入该技术。用户使用浏览器收发电子邮件。

□ 用户代理是普通的浏览器，用户和其远程邮箱之间的通信通过HTTP进行：

✓ 发件人使用**HTTP** 将电子邮件报文从其浏览器发送到其邮件服务器上；

✓ 收件人使用**HTTP**从其邮箱中取一个报文到浏览器；

□ 邮件服务器之间发送和接收邮件时，仍使用SMTP。

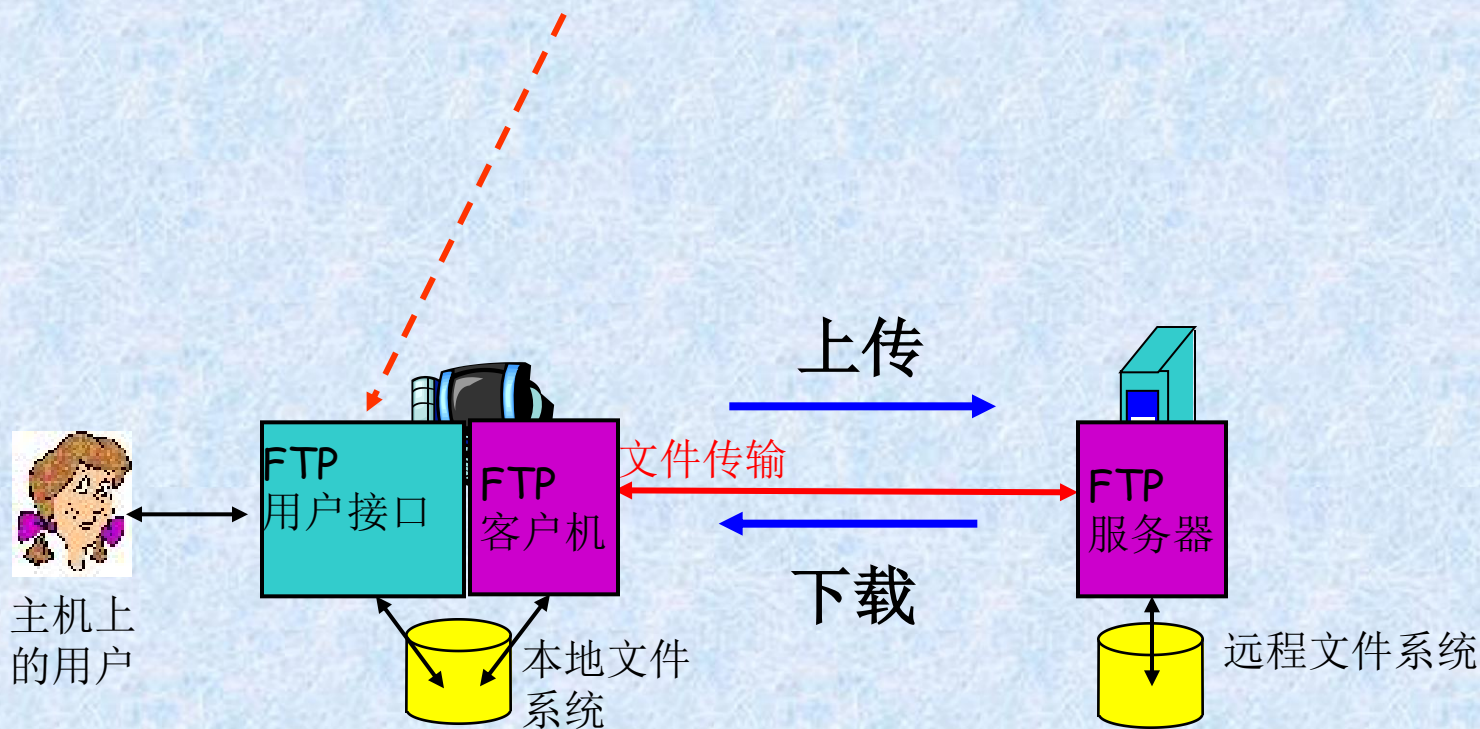
□ 用户可以在远程服务器上以层次目录方式组织报文。

如，Hotmail、Yahoo、Mail等。

2.4 文件传输协议：FTP

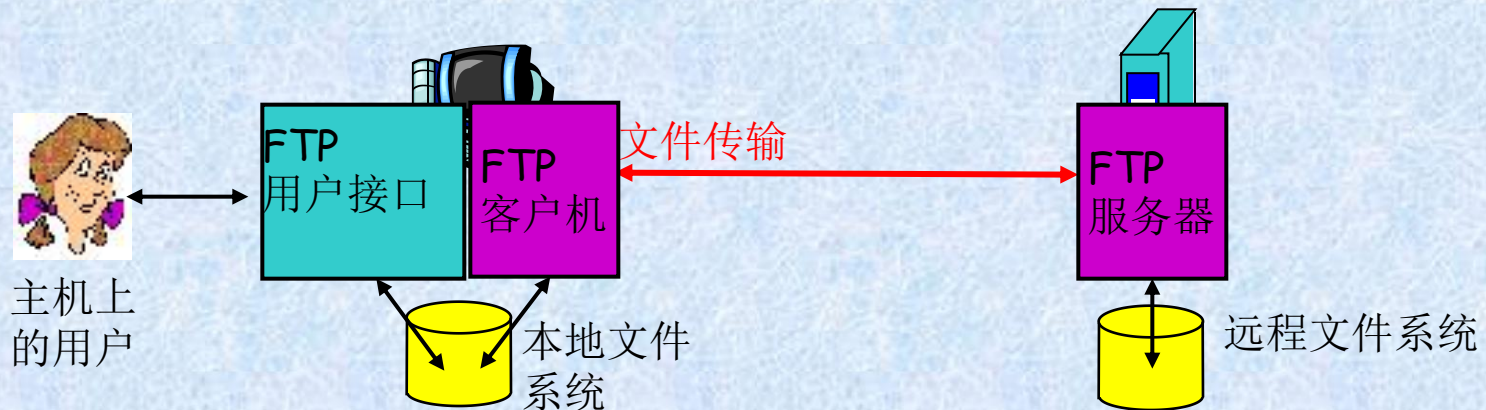
本地主机上的用户，向远程主机上传或者下载文件。

- ✓ 用户通过一个FTP用户代理与FTP服务器交互。



文件传输过程

- ✓ 用户提供远程主机的主机名：在本地主机的FTP客户机进程与远程主机FTP服务器进程之间**建立TCP连接**；
- ✓ 提供用户标识和口令：在该TCP连接上向服务器传送。
- ✓ 服务器验证通过后，进行文件传送（双向）：
将本地文件系统中的文件传送到远程文件系统（**上传**）
或从远程文件系统中得到文件（**下载**）

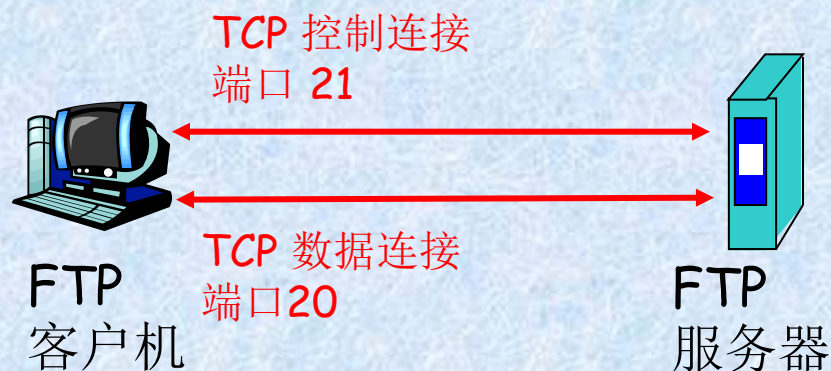


FTP与HTTP比较

都是文件传输协议，并运行在TCP上。

✓ *FTP使用了两个并行的TCP连接:*

- ◆ 控制连接:
- ◆ 数据连接:



控制连接

用于在两主机间**传输控制信息**（如用户标识、口令等）

- ✓ FTP会话开始前，FTP的客户机与服务器在**21号端口**上建立。
- ✓ FTP的客户机通过该连接发送用户标识和口令，或改变远程目录的命令。



数据连接

用于准确传输文件。

- ✓ 当服务器收到一个文件传输的命令后(从远程主机上读或写)，在20端口发起一个到客户机的数据连接。
- ✓ 在该数据连接上传送一个文件并关闭连接。
- 控制连接是持续的：在整个用户会话期间一直保持；
- 数据连接是非持续的：会话中每进行一次文件传输，都需要建立一个新的数据连接。



✓ *FTP*的控制信息是带外传送（out-of-band）：

使用分离的控制连接；

*HTTP*的控制信息是带内传输(in-band)：

请求和响应都是在传输文件的TCP连接中发送。

✓ *FTP*协议是有状态的：

*FTP*服务器对每个活动用户会话的状态进行追踪，并保留；限制同时会话的总数。

*HTTP*协议是无状态的：不对用户状态进行追踪。

2.5 DNS: 因特网的目录服务

□ 标识主机的两种方式:

✓ **主机名**: 由不定长的字母和数字组成。便于记忆。

如 www.yahoo.com

路由器处理困难。

✓ **IP地址**: 由4个字节组成, 有着严格的层次结构。

路由器容易处理。

如IP地址 (点分十进制): 121.7.106.83

网络号 主机号

2.5.1 DNS提供的服务

报文在网络中传输，使用IP地址。

- 域名系统DNS (*Domain Name System*): 进行主机名到IP地址的转换。
- ✓ 一个由分层的DNS服务器实现的分布式数据库
- ✓ 允许主机查询分布式数据库的应用层协议;

说明

- ✓ 运行BIND软件的UNIX机器；
- ✓ DNS协议运行在UDP之上，使用53号端口。
- ✓ DNS通常直接由其他的应用层协议 (包括HTTP、SMTP 和FTP)使用，以将用户提供的主机名解析为IP地址。用户只是间接使用。

□ 例，某个用户主机上的一个浏览器访问某个Web页，
`www.someschool.edu/index.html`

用户主机要**将一个HTTP请求报文发送到Web服务器**
`www.someschool.edu`，需先得到相应的IP地址。

□ 过程如下：

- ✓ 用户主机上运行 DNS应用的客户机端。
- ✓ 浏览器从URL中解析出主机地址，传给DNS客户机端。
- ✓ DNS客户机向DNS服务器发送一个包含主机名的请求；
- ✓ DNS客户机收到含有对应主机名的IP地址的回答报文；
- ✓ 浏览器向该IP地址指定的HTTP服务器发起一个TCP连接。

增加一定时延。

DNS服务

❑ 主机名到IP地址的转换

❑ 主机别名

- 规范名和别名：通过DNS可以得到主机别名(别名更易记)对应的规范主机名及IP地址。

❑ 邮件服务器别名

- 电子邮件应用程序调用DNS，对提供的邮件服务器别名进行解析，以获得该主机的规范主机名及其IP地址。

❑ 负载分配

- 冗余服务器：一个IP地址集合和一个规范主机名

2.5.2DNS工作机理概述

□ DNS工作过程

1. 某个应用程序调用DNS的客户端，并指明需要被转换的主机名
2. 用户主机上的DNS客户端接收到后，向网络中发送一个DNS查询报文
3. 经过若干毫秒到若干秒的时延后，用户主机上的DNS客户端接收到一个提供所希望映射的DNS回答报文
4. 映射结果被传递到调用DNS客户端的应用程序

DNS查询/回答报文使用UDP数据报，从53号端口发送

从用户主机调用应用程序的角度看，DNS是一个提供简单、直接的转换服务的黑盒子。

DNS的一种简单设计 (集中式设计)

- 假设因特网上只使用一个DNS服务器，该服务器包含所有的映射。
- 工作过程：
 1. 用户直接将所有查询直接发往单一的DNS服务器
 2. 该DNS服务器直接对所有的查询客户做出响应

□ **优点：**设计简单，具有吸引力

□ **问题：**

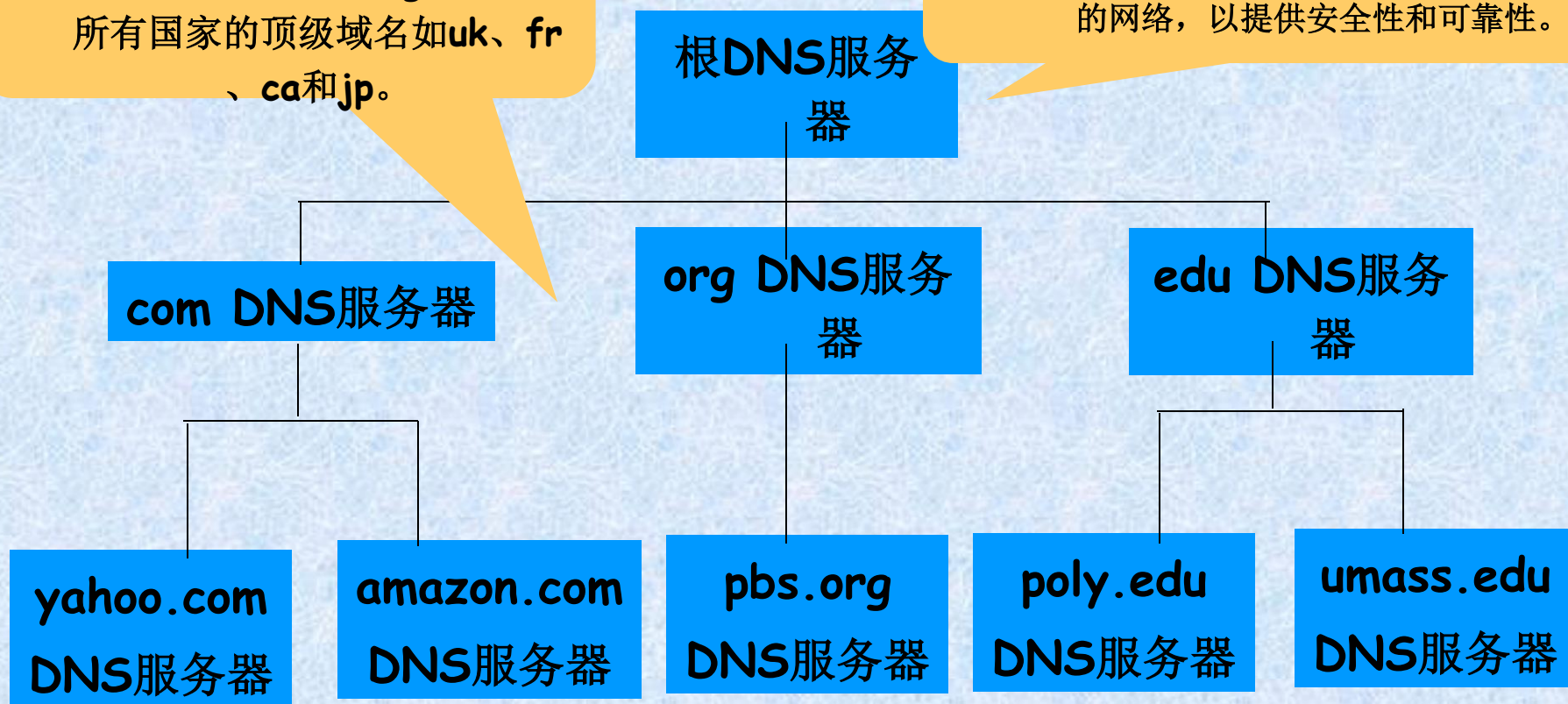
1. **单点故障：**若该DNS服务器崩溃，整个因特网随之瘫痪。
2. **通信容量：**单个DNS服务器要处理所有的DNS查询。
3. **远距离的集中式数据库：**单个DNS服务器不可能“邻近”所有查询客户，远距离查询将导致严重时延。
4. **维护：**单个DNS服务器要为所有的因特网主机保留记录。

1.分布式、层次数据库

- 单一DNS服务器上运行集中式数据库完全没有可扩展能力
- 为了处理扩展性问题，DNS使用了大量的DNS服务器，它们以层次方式组织，并且分布在全世界范围内。
- 注意：
 - 没有一台DNS服务器拥有因特网上所有主机的映射
 - 该映射分布在所有的DNS服务器上

顶级域（TLD）DNS服务器：负责顶级域名如**net**、**gov**，以及所有国家的顶级域名如**uk**、**fr**、**ca**和**jp**。

因特网上有**13个根DNS服务器**（标号为**A到M**），每台服务器实际上是一个冗余服务器的网络，以提供安全性和可靠性。



DNS服务器的部分层次结构

权威DNS服务器：在因特网上具有公共可访问主机的组织机构用来保存将主机名映射为**IP地址**的**DNS**记录。多数大学和大公司实现和维护它们基本和辅助的权威**DNS**服务器。

3种类型的DNS服务器交互的方式

- 假定一个DNS客户要决定主机名www. amazon. com的IP地址。
 1. 客户首先与根服务器之一联系，它将返回顶级域名com的TLD服务器的IP地址
 2. 该客户则与这些TLD服务器之一联系，它将为amazon. com返回权威服务器的IP地址。
 3. 最后，该客户与amazon. com权威服务器之一联系，它为主机名www. amazon. com返回其IP地址。

本地DNS服务器 (local DNS server)

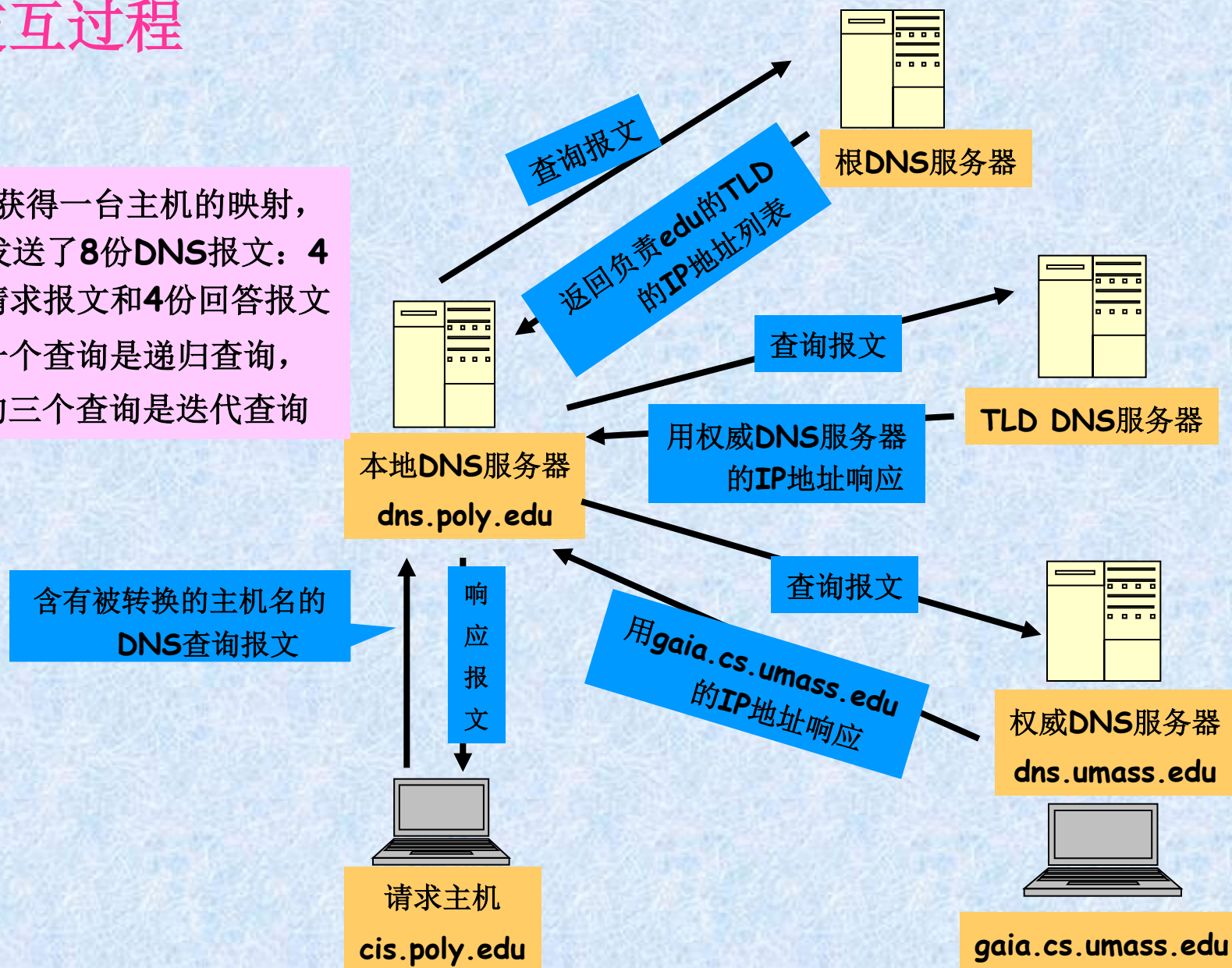
1. 严格来说，不属于DNS服务器的层次结构
2. 每个ISP都有一台本地DNS服务器（也叫**默认DNS服务器**）
3. 主机的本地DNS服务器**通常“邻近”本主机**
4. 当主机发出DNS请求时，该请求被发往本地DNS 服务器，它起着代理的作用，并将该请求转发到DNS服务器层次结构中。

□ 例：

- ✓ 假设主机 **cis.poly.edu** 想知道主机 **gaia.cs.umass.edu** 的 **IP** 地址。
- ✓ 同时假设理工大学的本地 **DNS** 服务器为 **dns.poly.edu**，并且 **gaia.cs.umass.edu** 的权威 **DNS** 服务器为 **dns.umass.edu**

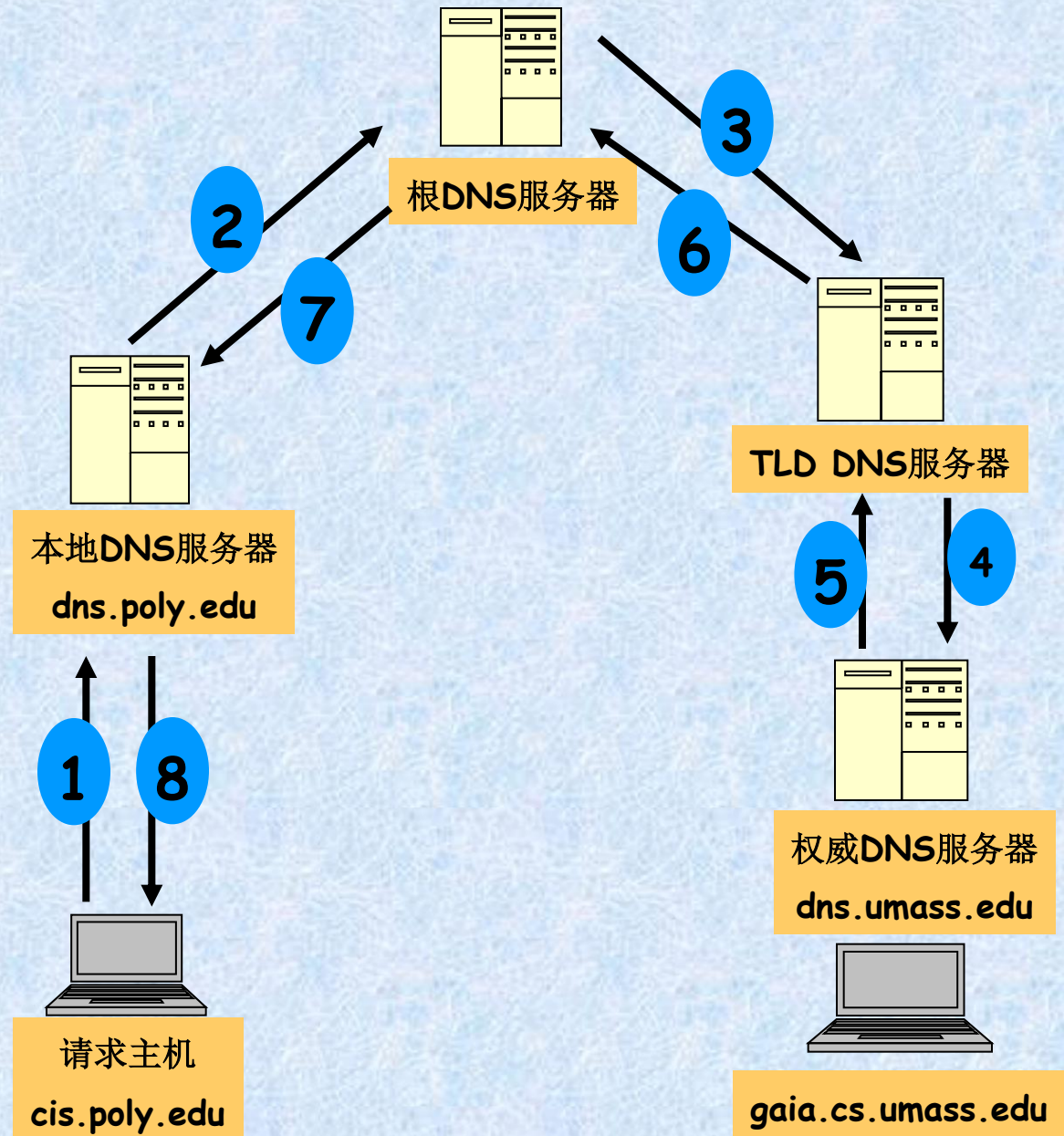
交互过程

1. 为了获得一台主机的映射，共发送了**8份DNS报文**：**4份请求报文**和**4份回答报文**
2. 第一个查询是递归查询，后继的三个查询是迭代查询



DNS中的递归查询

1. 从理论上讲，任何**DNS**查询既可以是迭代的也能是递归的。
2. 一般的，从请求主机到本地**DNS**服务器的查询是递归的，其余的查询是迭代的



2.DNS缓存

□ 作用

改善时延性能、减少在因特网上到处传输的DNS报文数量

□ 原理

在一个请求链中，当某DNS服务器接收一个DNS回答时，它将该回答中的信息缓存在本地存储器中。

□ 注意

由于主机和主机名与IP地址间的映射并不是永久的，DNS服务器在一段时间后（通常设置为两天）将丢弃缓存的信息。

□ 举例：

1. 假定主机 `apricot.poly.edu` 向 `dns.poly.edu` 查询主机名 `cnn.com` 的IP地址
2. 假定过了几个小时，理工大学的另外一台主机也向 `dns.poly.edu` 查询相同的主机名
3. 因为有了缓存，该本地DNS服务器可以立即返回 `cnn.com` 的IP地址，而不必查询其他任何DNS服务器。

2.5.3 DNS记录报文

- **资源记录 (RR)**：由DNS服务器储存，提供了主机名到 IP地址的映射。

(每个DNS回答报文包含了一条或多条资源记录)

资源记录是一个包含了下列字段的4元组：

(Name, Value, Type, TTL)

该记录的生存时间，决定了资源记录应当从缓存中删除的时间。

记录例子（忽略TTL）

Name和Value的值取决于Type:

- Type=A, Name则是主机名, Value是该主机对应的IP地址。提供了标准的主机名到IP地址的映射。
(relay1.bar.foo.com, 145.37.93.126, A)
- Type=NS, Name是一个域（如foo.com）, Value是个知道如何获得该域中主机IP地址的权威DNS服务器主机名。
该记录用于沿着查询链来路由DNS查询。
(foo.com, dns.foo.com, NS)

□ Type=CNAME, Value是别名为Name的主机对应的规范主机名。
向查询的主机提供一个主机名对应的规范主机名。
(foo.com, relay1.bar.foo.com, CNAME)

□ Type=MX, Value是别名为Name的邮件服务器的规范主机名。
(foo.com, mail.bar.foo.com, MX) MX记录允许邮件服务器主机名具有简单的别名。

注意：通过使用MX记录，一个公司的邮件服务器和其他服务器（如Web服务器）可以使用相同的别名

- 例：假设一台edu TLD服务器不是主机gaia.cs.umass.edu的权威DNS服务器，则该服务器将包含一条包括主机cs.umass.edu的域记录，如（umass.edu, dns.umass.edu, NS）；还将包含一条类型A记录，如（dns.umass.edu, 128.119.40.111, A），该记录将名字dns.umass.edu映射为一个IP地址。

服务器不是用于某主机名的权威服务器，则该服务器会有一条类型NS记录，该记录对应于包含主机名的域；还将包含一条类型A记录

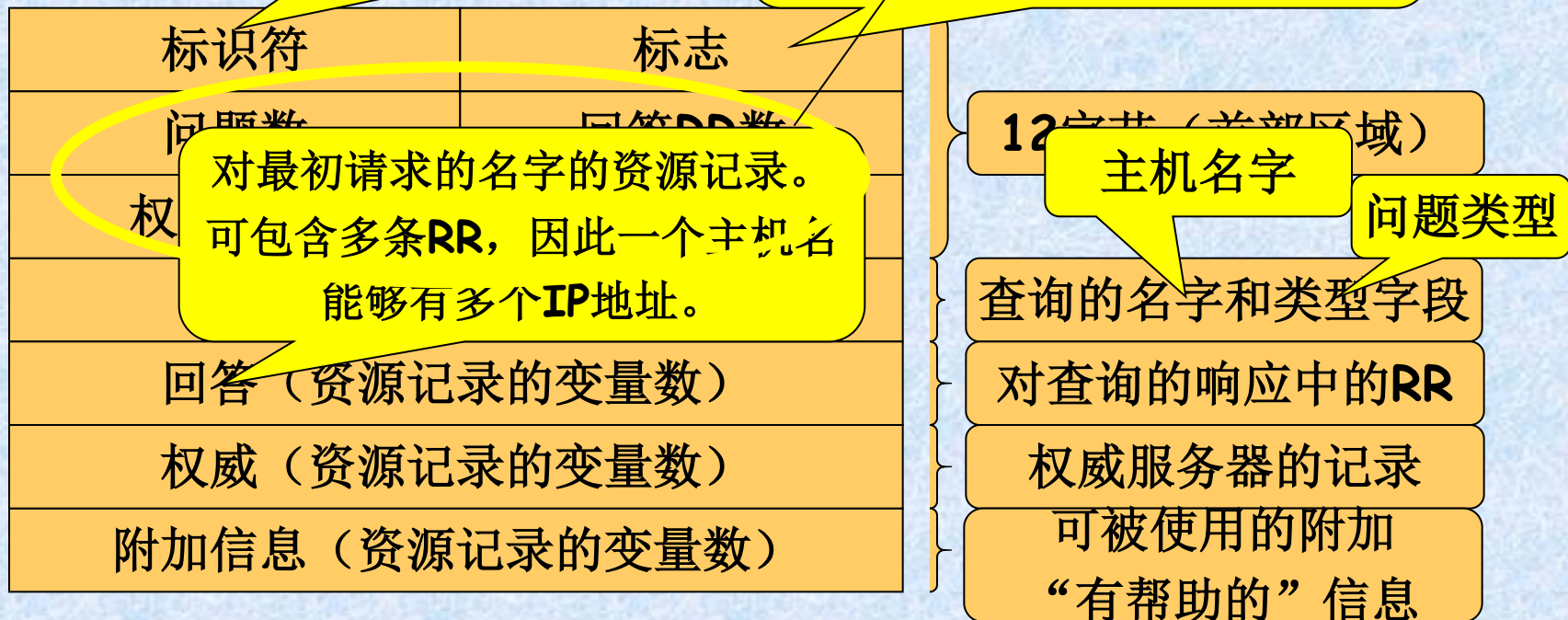
1.DNS报文

包含查

16bit，用于标识该查询，会被复制到对查询的回答报文中，以便让客户端匹配发送的请求和接收到

指出在首部后的4类数据区域出现的数量

标志字段：含有若干标志。
1比特的“查询/回答”标志位。
查询报文——0；回答报文——1。



2. 在DNS数据库中插入记录

是一个商业实体，它验证该域名的唯一性，
将该域名输入DNS数据库，对提供的服务收取少量费用

例：创建网络乌托邦（Network Utopia）公司

- ❑ 向注册登记机构注册域名networkutopia.com，需要向机构提供基本和辅助权威DNS服务器的名字和IP地址。该名字和IP地址是dns1.networkutopia.com和dns2.networkutopia.com及212.212.212.1和212.212.212.2。
- ❑ 对于用于networkutopia.com的每个权威服务器，该注册登记机构将下列两条资源记录输入TLD com服务器：
 - (networkutopia.com, dns1.networkutopia.com, NS)
 - (dns1.networkutopia.com, 212.212.212.1, A)
 - (networkutopia.com, dns2.networkutopia.com, NS)
 - (dns2.networkutopia.com, 212.212.212.2, A)
- ❑ 确保A记录和MX记录输入权威DNS服务器中。

总结例子： 澳大利亚的Alice观看www.networkutopia.com的Web页面

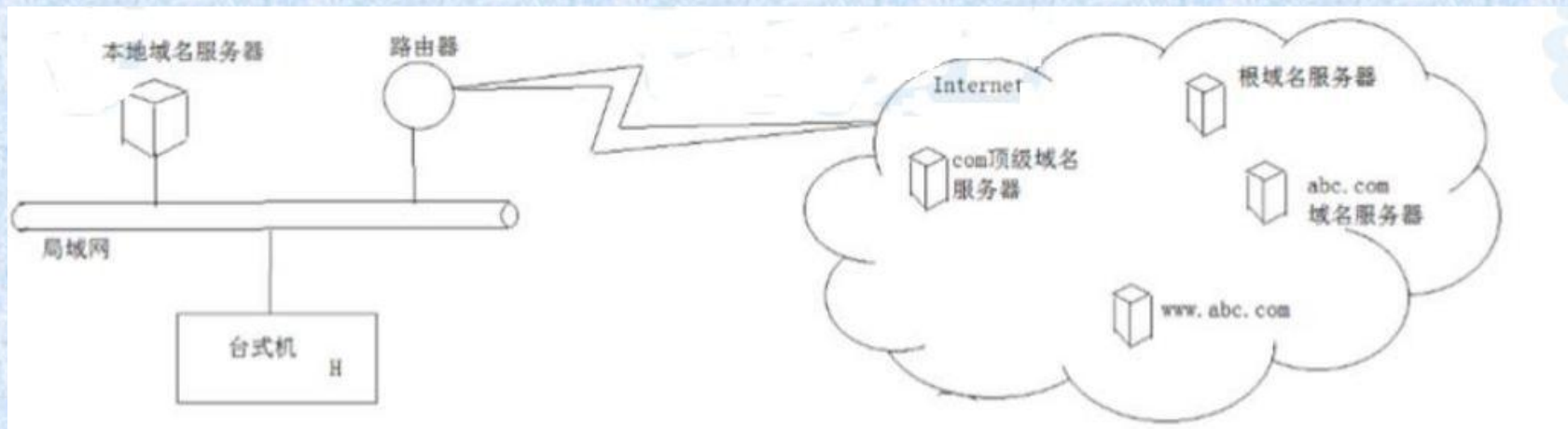
1. Alice主机向本地DNS服务器发送请求。
2. 本地服务器接着联系一个TLD com服务器。（如果TLD com服务器地址没有被缓存，该本地DNS服务器也将必须与根DNS服务器相联系。）
3. 该TLD com服务器包含前面列出的类型NS和类型A资源记录，向Alice的本地DNS服务器发送一个回答，该回答包含这两条资源记录。
 - networkutopia.com, 权威服务器DNS名字, NS
 - 权威服务器DNS名字, 212.212.212.1, A
1. 该本地DNS服务器向212.212.212.1发送一个DNS查询，请求应对与www.networkutopia.com（212.212.71.4）的类型A记录。
2. Alice的浏览器此时能够向主机212.212.71.4发起一个TCP连接，并在该连接上发送一个HTTP请求。

1、无需转换即可由SMTP协议直接传输的内容是

- ☐ A JPEG图像
- ☐ B MPEG视频
- ☐ C EXE文件
- ☒ D ASCII文本

提交

2、假设下图所示网络中的本地域名服务器只提供递归查询服务，其他域名的服务器均只提供迭代查询服务：局域网内主机访问Internet上各服务器的往返时延（RTT）均为10ms，忽略其他各种时延，若主机H通过超链接<http://www.abc.com/index.html>，请求浏览纯文本Web页index.html，则从点击超链接开始到浏览器接收到index.html页面为止，所需最短、最长时间分别是：



A 10ms,40ms

B 10ms,50ms

C 20ms,40ms

D 20ms,50ms

提交