第七章 应用层

课前思考

- 什么是应用层协议？
- 什么是域名系统（DNS）？
- 什么是URL?
- WWW基本要素是什么?
- 电子邮件是怎么工作的？

7.1 应用层概述

很多应用系统的完成需要依靠位于不同端（主机）系统中进程之间的相互通信和协同。

事实上，计算机网络系统的出现及发展本身就是为了实现不同端系统之间的信息交互和协同。

7.1.1 基本概念

1. 应用层与应用层协议

在TCP/IP中，应用层对应OSI/RM中的会话层、表示层和应用层，是应用程序与网络传输的接口，是面向应用需求的通信协议中的最高端。

应用层协议不是应用程序，也不解决用户的具体应用需求，而是为应用程序进程的网络通信提供服务的第一层协议，是为用户的应用需求提供通信服务。

根据服务的对象，应用层协议可分为公共的标准协议和私有的非标准化协议。其中，公共协议是为一类应用程序提供通信服务，私有协议则是为某个具体应用提供通信服务。

应用层协议为具体应用程序的需求提供通用的、标准化的通信平台，以沟通传输层及其以下网络层次的网络通信协议。

因此，应用层协议定义了运行在不同端系统上的应用程序进程相互传递报文的规范。这些规范一般包括：

- 交换的报文类型，如请求报文和响应报文
- 语法，如报文中的各个字段及这些字段的描述规范
- 语义，即报文各字段的可能取值及其含义
- 进程何时、如何发送报文及对报文进行响应。

2. 应用层协议的体系架构

（1）客户-服务器模式

- 服务器：需要具备7*24小时提供服务的能力，拥有可永久访问地址/域名，以及拥有良好的可扩展性。
- 客户端：可以间歇性进入网络，客户端之间通常不直接连接。

在这种模式下：

- 客户：提出需求，并完成预期的行为。
- 服务器：管理和调度资源，满足客户对资源的利用。
- 交互：在协议的约束下，避免客户申请与服务器调度之间的冲突。

（2）P to P模式

- 对等性：通信的各方地位平等，互为客户端也互为服务器。
- 独立性：对中心服务器依赖最小（甚至没有）。应用程序在间歇性连接的主机之间直接通信，相互提供对方需要的服务。

在这种模式下：

- 端系统：不需要随时在线，且任意端系统均可直接通信。
- 自治性：没有中心节点协调，各端系统之间平等协商。
- 生存能力：即使有部分端系统退出，网络依然生存。

（3）混合模式

一种混合了C/S和P2P的通信模式，兼具二者特点。

通常是：

- 服务器：负责全局性的服务，如搜索等。
- 客户端：负责提供具体的服务。

3. 对传输层的要求

不同的应用程序，对传输层有不同的要求。有些对时间敏感，有些对数据敏感。

（1）可靠数据传输

- 如果能够确保数据交付，则这样的协议就认为是提供了可靠数据传输（Reliable Data Transfer）。
- 有些应用程序要求确保可靠性，而也有些应用程序能够容忍一定程度的数据丢失(Loss-Tolerant Application，容忍丢失应用），如多媒体应用。

（2）吞吐量

可用吞吐量是指发送进程能够向接收进程交付比特的速率。

- 具有吞吐量要求的应用程序被称为带宽敏感应用(Bandwidth-Sensitive Application)，许多多媒体应用是带宽敏感度。
- 弹性应用（Alastic Application）则能够根据情况或多或少地利用可供使用的吞吐量。电子邮件、文件传输以及Web传送都属于弹性应用。

（3）定时

能够确保发送方注入进套接字中的每个比特到达接收方的套接字不迟于某个预期的时间（如100ms）。这些服务对交互式实时应用程序有吸引力。

- 在网络电话中，较长的时延会导致会话出现不自然的停顿；在游戏中，较长的时延使得它失去真实感。

（4）安全性

可以提供一种或多种安全性服务。

几种常见应用对网络的要求

应用	数据敏感	带宽敏感	时间敏感
文件传输	是	弹性	不
电子邮件	是	弹性	不
Web文档	是	弹性（几bps）	不
网络电话/视频会议	容忍	音频（几kbps-1Mbps）， 视频（10kbps-5Mbps）	是，<100ms
音视频存储	容忍	同上	是，数秒
交互式游戏	容忍	几kbps-10kbps	是，<100ms
即时通信	是	弹性	不确定

- **TCP服务**
  - 面向连接的服务，全双工
  - 可靠的数据传送服务：无差错，按适当顺序交付所有发送的数据
  - 拥塞控制机制：当发送方和接收方之间的网络出现拥塞时，TCP会抑制发送进程
  - 安全套接字层 SSL 提供安全性服务
- **UDP服务**
  - 提供最小服务
  - 无连接
  - 不可靠数据传送服务

在TCP/IP的传输层协议中不提供吞吐量和定时服务

4.TCP/IP中的应用层协议

TCP/IP协议簇提供了一些常用的公共应用层协议。

- 域名解析协议
- 电子邮件协议
- 文件传输协议
- 超文本传输协议
- 会话发起协议
- 远程访问协议

7.2 域名解析协议

域名解析协议，有很多别称，如因特网的目录服务、域名服务、域名系统（Domain Name System，DNS）等，常常用简称DNS替代。

DNS用来解决主机名与IP地址的映射关系，使互联网用户无需记忆相对难于记忆的IP地址，而只要记住更加接近人类理解特性的域名即可。

因此，互联网用户对DNS有极强的依赖性。

7.2.1 域名系统概述

1. 域名及域名结构

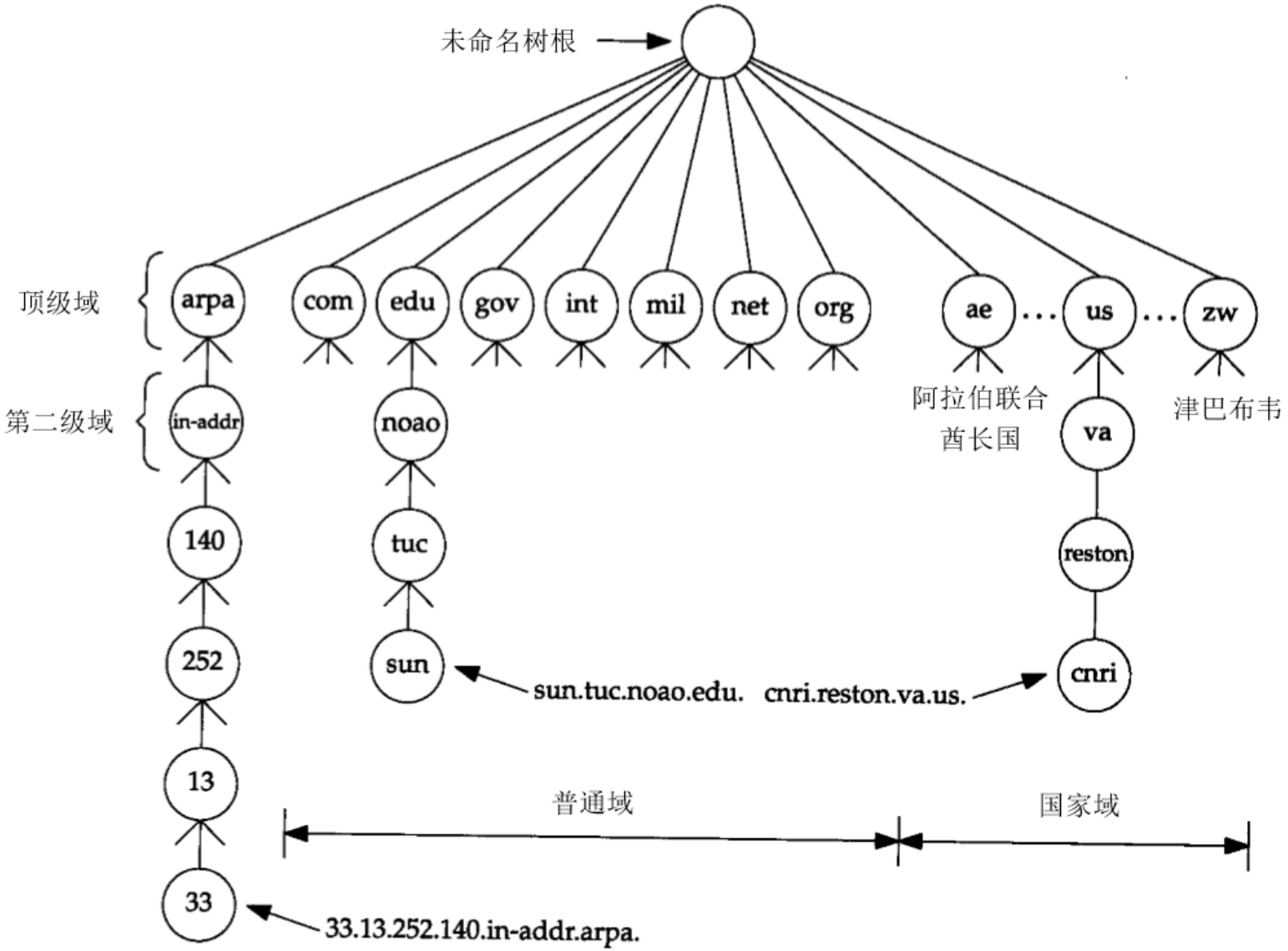
通过采用层次结构的命名方法确保域名的唯一性，从而可以唯一的指明某个域名对应的主机的IP地址。

按照层次结构，域名分为：

- 顶级域名
- 二级域名
- 三级域名
- 四级域名

⋮

附：因特网的域名空间


未命名树根
顶级域
第二级域
arpa
com
edu
gov
int
mil
net
org
ae
us
zw
阿拉伯联合
酋长国
津巴布韦
in-addr
noao
va
140
tuc
reston
252
sun
cnri
sun.tuc.noao.edu.
cnri.reston.va.us.
13
普通域
国家域
33
33.13.252.140.in-addr.arpa.

域名：每一个域名（英文域名）都是一个标号序列（labels），用字母（A-Z，a-z，大小写等价）、数字（0-9）和连接符（-）组成，标号序列总长度不能超过255个字符。

域名结构：由点号分割成一个个的标号（label），每个标号应该在63个字符之内，每个标号都是其所在层次的域名。级别最低的域名自左至右逐步上升。

…．三级域名．二级域名．顶级域名.

绝对域名

以点“.”结尾的域名称为绝对域名或完全合格的域名（**Full Qualified Domain Name，FQDN**），不以点结尾，则是不完全的域名。

- 如果不完全的域名是由两个或两个以上的标号组成，则认为是完全域名；
- 如果在不完全的域名右部连接一个局部后缀，也认为是完全域名。

- 域名只是个逻辑概念，并不代表计算机所在的物理地点。
- 变长的域名和使用有助记忆的字符串，是为了便于人来使用。而 IP 地址是定长的 32 位二进制数字则非常便于机器进行处理。
- 域名中的“点”和点分十进制 IP 地址中的“点”并无一一对应的关系。点分十进制 IP 地址中一定是包含三个“点”，但每一个域名中“点”的数目则不一定正好是三个。

2. 顶级域名 TLD (Top Level Domain)

（1）通用域名

通用域名共有7个，均为三个字节长度，分别是.com、.net、.org、.edu、.gov、.mil、.int

其中，.gov、.mil两个顶级域名为美国专用，.edu基本只有美国的教育机构使用

其余的通用域名全世界各国均可使用

（2）国家域名

基于ISO 3166中定义的国家代码设计的顶级域名，这些域被称为国家域或地理域，均为2个字节长度

例如：**cn**（中国大陆）、**de**（德国）、**eu**（欧盟）、**jp**（日本）、**hk**（香港）、**tw**（台湾）、**uk**（英国）、**us**（美国）。

（3）arpa域

这种顶级域名只有一个，即 **arpa**，用于反向域名解析，因此又称为反向域名。

（4）新增通用顶级域名

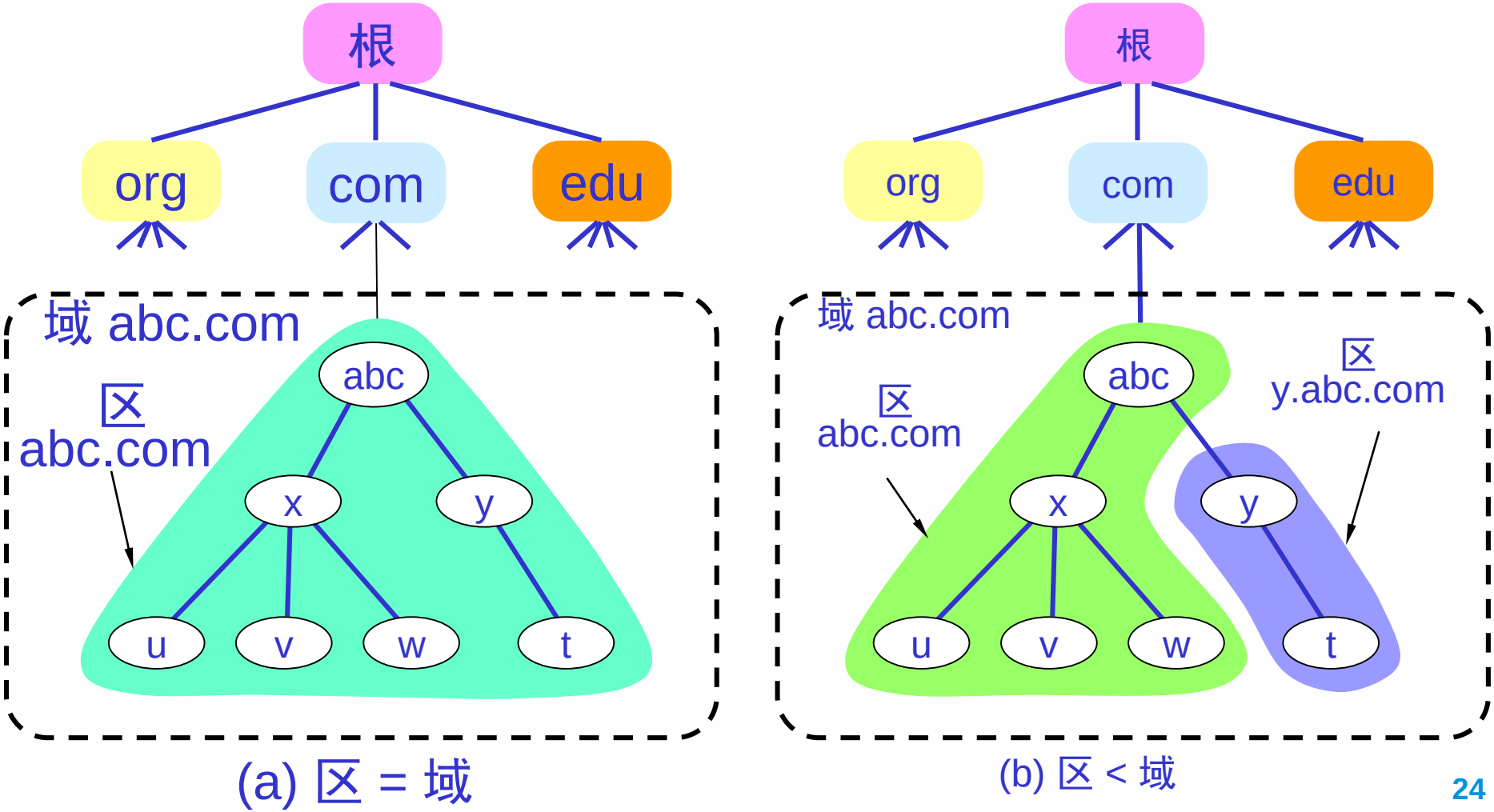
- .aero （航空运输企业）
- .biz （公司和企业）
- .cat （加泰隆人的语言和文化团体）
- .coop （合作团体）
- .info （各种情况）
- .jobs （人力资源管理者）
- .mobi （移动产品与服务的用户和提供者）
- .museum （博物馆）
- .name （个人）
- .pro （有证书的专业人员）
- .travel （旅游业）

3. 域名服务器

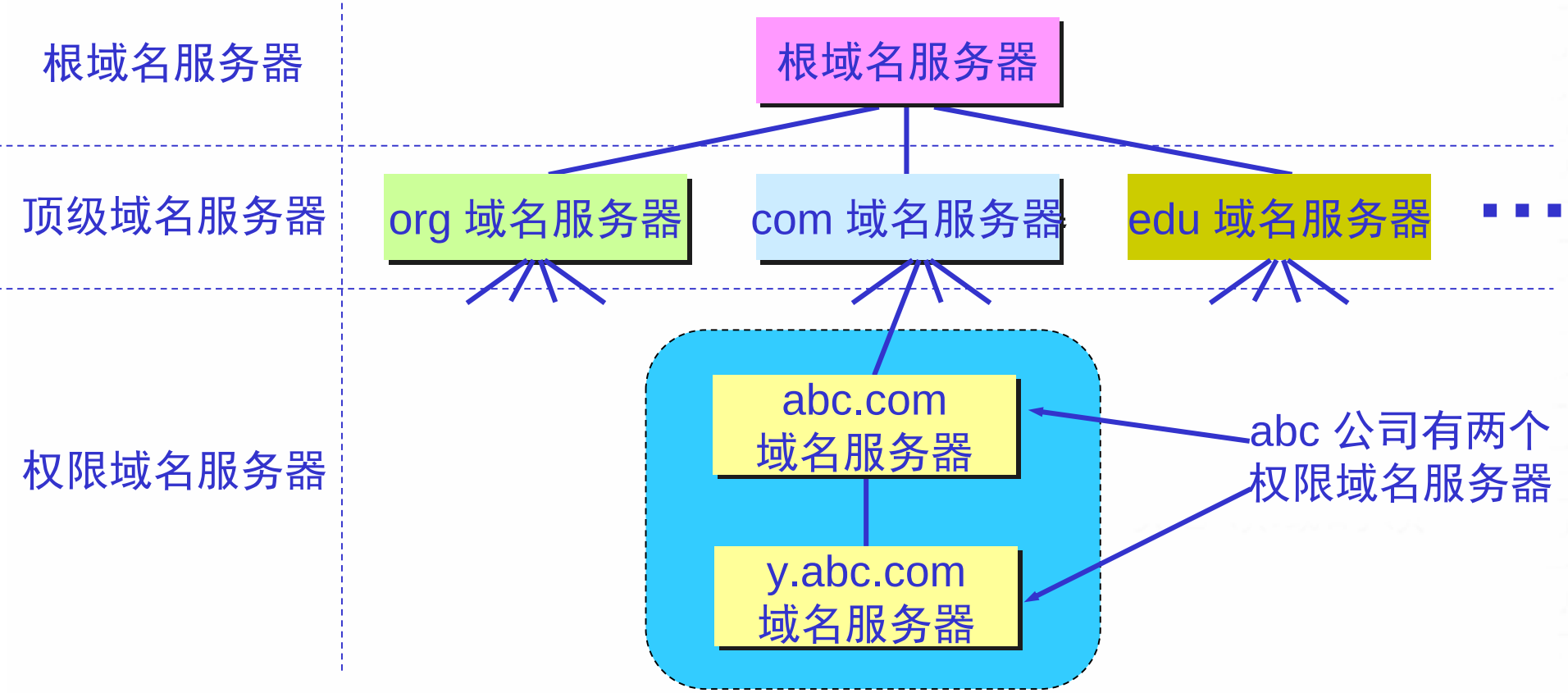
域名需要由遍及全世界的域名服务器去解析，域名服务器实际上就是装有域名系统的主机。

- 一个服务器所负责管辖的（或有权限的）范围叫做区(zone)。
- 各单位根据具体情况来划分自己管辖范围的区。但在一个区中的所有节点必须是能够连通的。
- 每一个区设置相应的权限域名服务器，用来保存该区中的所有主机的域名到IP地址的映射。
- DNS 服务器的管辖范围不是以“域”为单位，而是以“区”为单位。

区的不同划分方法


根
org
com
edu
域 abc.com
区
abc.com
abc
x
y
u
v
w
t
(a) 区 = 域
根
org
com
edu
域 abc.com
区
abc.com
区
y.abc.com
abc
x
y
u
v
w
t
(b) 区 < 域

树状结构的 DNS 域名服务器



域名服务器分类

根域名服务器
顶级域名服务器
权限域名服务器
本地域名服务器

这些域名服务器由ICANN（互联网名称和数字地址分配公司）授权的各种组织负责管理维护。

根域名服务器

最高层次的域名服务器。

- 根域名服务器是最重要的域名服务器。所有的根域名服务器都知道所有的顶级域名服务器的域名和 IP 地址。
- 不管是哪一个本地域名服务器，若要对因特网上任何一个域名进行解析，只要自己无法解析，就首先求助于根域名服务器。
- 在因特网上共有13 个不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从a 一直到 m（前13 个字母）。

根域名服务器共有 13 套装置

- 这些根域名服务器相应的域名分别是

  a.rootservers.net

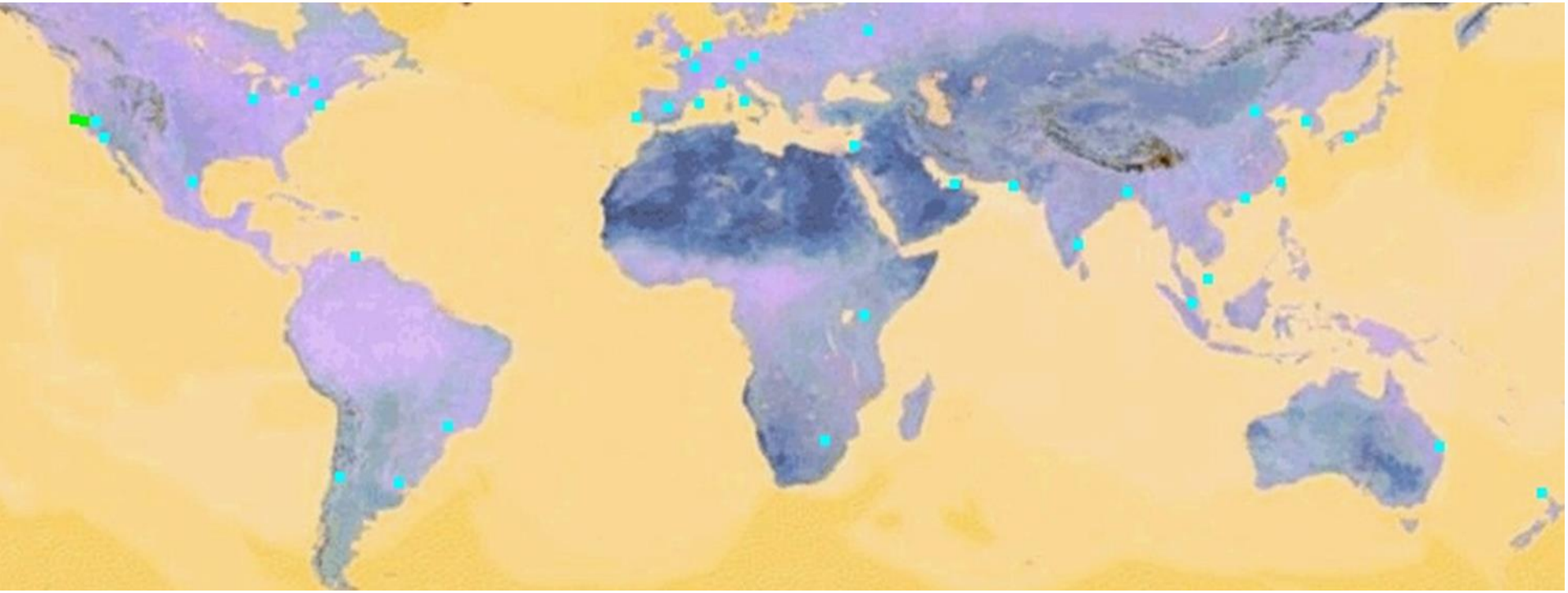
  b.rootservers.net

  …

  m.rootservers.net

- 1个主根（美国），12个辅根（9个在美国，2个在欧洲，1个在日本）
- 在世界各地安装了很多根域名服务器的镜像服务器并共享同一个 IP 地址，在中国有6组（F，I（3），J，L）服务器。
- 世界上大部分 DNS 域名服务器都能就近找到一个根域名服务器。

根域名服务器 f 的地点分布图（共有40多台）



顶级域名服务器

- 这些域名服务器负责管理在该顶级域名服务器注册的所有二级域名。
- 当收到 DNS 查询请求时，就给出相应的回答（可能是最后的结果，也可能是下一步应当找的域名服务器的 IP 地址）。

权限域名服务器

- 负责一个区的域名服务器。
- 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。

本地域名服务器

- 本地域名服务器对域名系统非常重要。
- 当一个主机发出 DNS 查询请求时，这个查询请求报文就发送给本地域名服务器。
- 每一个因特网服务提供者 ISP，或一个大学，甚至一个大学里的系，都可以拥有一个本地域名服务器，
- 这种域名服务器有时也称为默认域名服务器。

4. 域名服务器的可靠性

- DNS 域名服务器都把数据复制到几个域名服务器来保存，其中的一个是主域名服务器，其他的是辅助域名服务器。
- 当主域名服务器出故障时，辅助域名服务器可以保证 DNS 的查询工作不会中断。
- 主域名服务器定期把数据复制到辅助域名服务器中，而更改数据只能在主域名服务器中进行。这样就保证了数据的一致性。

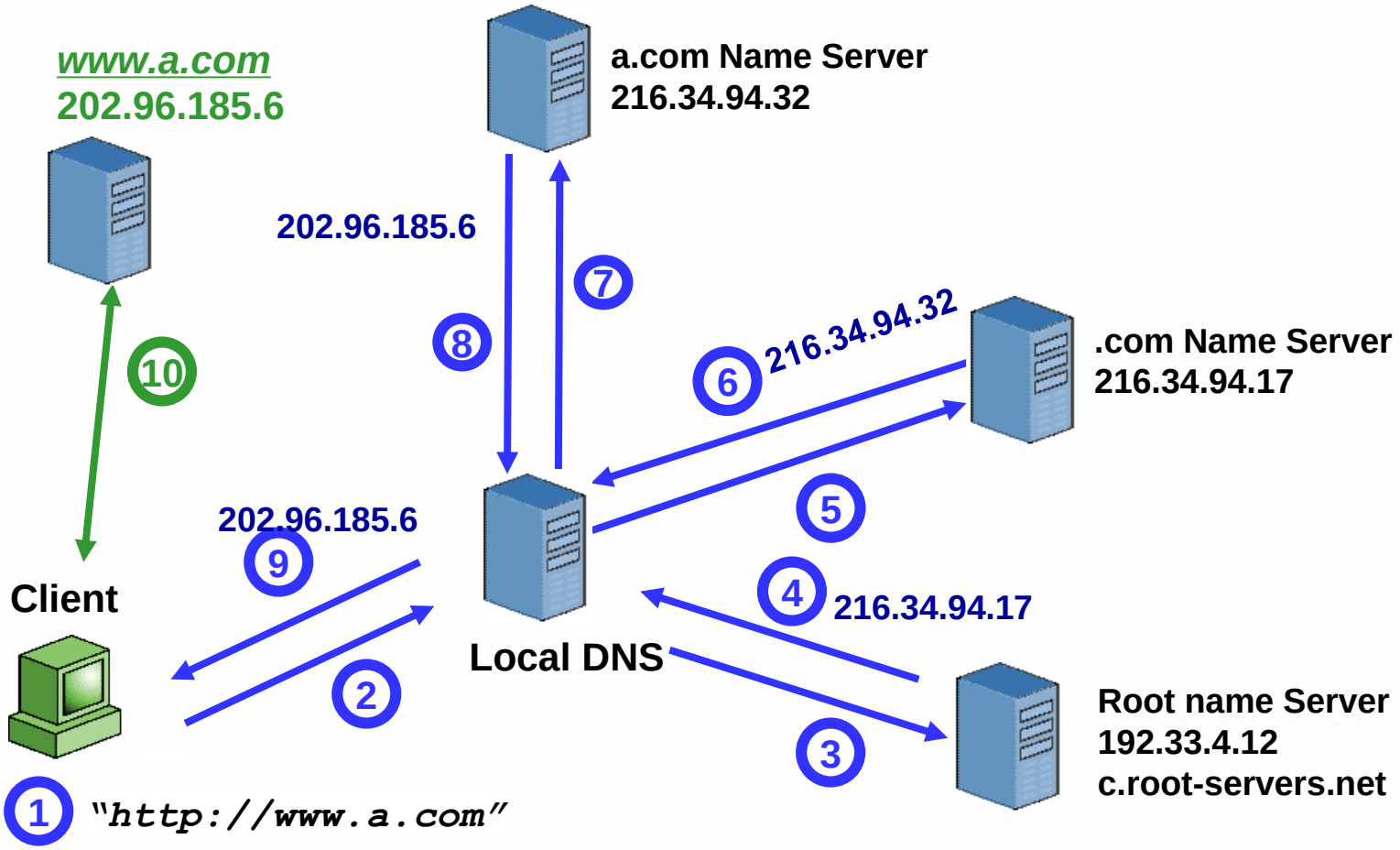
7.2.2 域名解析过程

1. 解析步骤

- 主机向本地域名服务器的查询一般都是采用递归查询。如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。
- 本地域名服务器向根域名服务器的查询通常是采用迭代查询。当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出所要查询的 IP 地址，要么告诉本地域名服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。

2. 解析过程

- 首先从主机本地Hosts文件查找。没找到就向本地DNS发出请求；
- 若本地DNS也找不到，则将请求发给负责该域的根域名字服务器，根服务器会返回一个相应的顶级域名服务器地址；
- 本地域名服务器向顶级域名服务器提出请求。顶级域名服务器会返回一个权限域名服务器地址；
- 本地域名服务器向权限域名服务器提出请求，权限域名服务器将返回目标域名的IP地址。
- 本地域名服务器向查询主机返回目标域名的IP地址。


www.a.com
202.96.185.6
a.com Name Server
216.34.94.32
202.96.185.6
7
8
10
6
216.34.94.32
.com Name Server
216.34.94.17
5
202.96.185.6
9
Client
4
216.34.94.17
Local DNS
2
3
Root name Server
192.33.4.12
c.root-servers.net
1
"http://www.a.com"

3. 名字的高速缓存

- 每个域名服务器都维护一个高速缓存，存放最近用过的名字以及从何处获得名字映射信息的记录。
- 可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报文的数量大为减少。
- 为保持高速缓存中的内容正确，域名服务器应为每项内容设置计时器，并处理超过合理时间的项（例如，每个项目只存放两天）。
- 当权限域名服务器回答一个查询请求时，在响应中都指明绑定有效存在的时间值。增加此时间值可减少网络开销，而减少此时间值可提高域名转换的准确性。

7.2.3 DNS的报文结构

DNS定义了用于查询和响应的报文格式。

由12字节的首部和4个长度可变的字段构成。


0
15
16
31
Transaction ID（会话标识）
Flags（标志）
Questions（问题数）
Answer RRs（回答 资源记录数）
Authority RRs（授权 资源记录数）
Additional RRs（附加 资源记录数）
Header
Queries（查询问题区域）
Answers（回答区域）
Authoritative nameservers（授权区域）
Additional recoreds（附加 区域）

1. DNS报文首部结构

（1）会话标识

是DNS报文的ID标识，对于请求报文和其对应的应答报文，这个字段是相同的，通过它可以区分DNS应答报文是哪个请求的响应

（2）标志

Flags	QR	opcode	AA	TC	RD	RA	(zero)	rcode
	1	4	1	1	1	1	3	4

QR（1bit）	查询/响应标志，0为查询，1为响应
opcode（4bit）	0表示标准查询，1表示反向查询，2表示服务器状态请求
AA（1bit）	表示授权回答
TC（1bit）	表示可截断的
RD（1bit）	表示期望递归
RA（1bit）	表示可用递归
rcode（4bit）	表示返回码，0表示没有差错，3表示名字差错，2表示服务器错误（Server Failure）

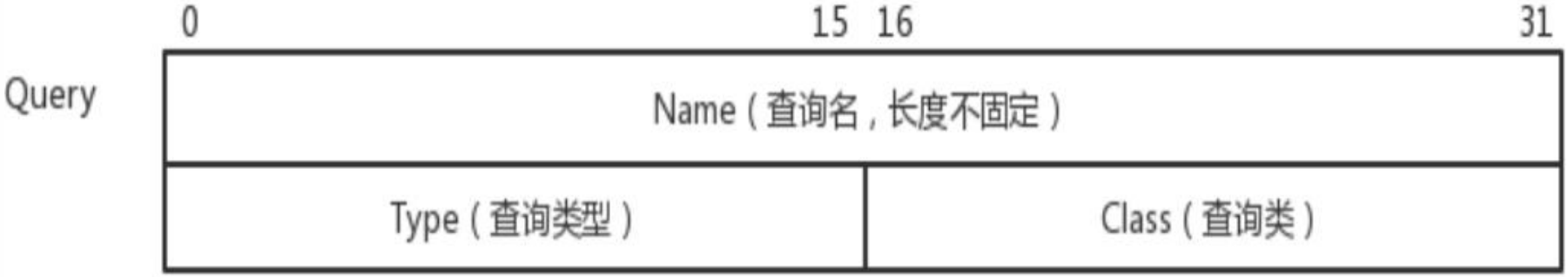
（3）四个数量

Questions、Answer RRs、Authority RRs、Additional RRs 各自表示后面的四个区域的数目。

- Questions表示查询问题区域节的数量
- Answers表示回答区域的数量
- Authoritative namesversers表示授权区域的数量
- Additional recoreds表示附加区域的数量

2. DNS报文正文

（1）Queries区域



- 查询名：长度不固定，且不使用填充字节，一般该字段表示的就是需要查询的域名（如果是反向查询，则为IP，反向查询即由IP地址反查域名）。

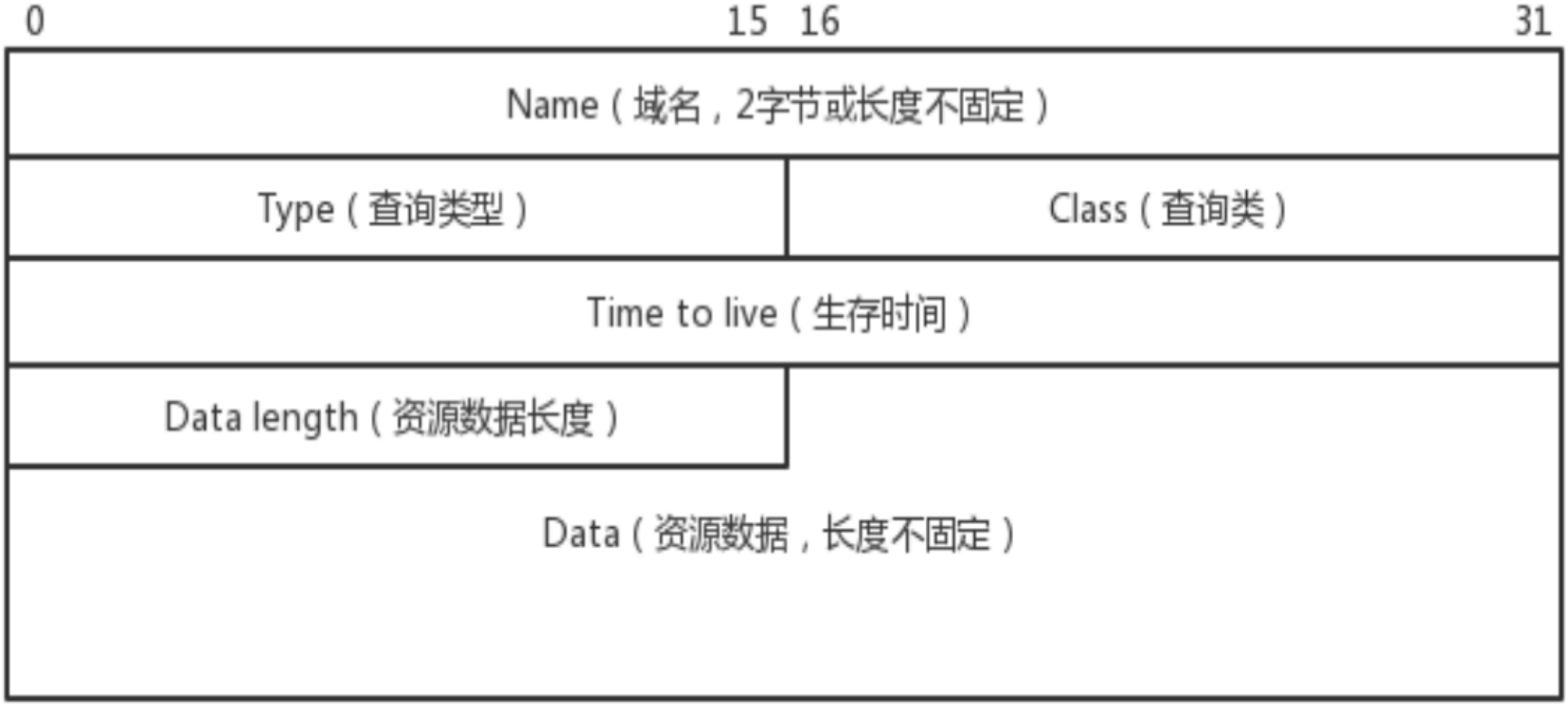
查询类型

类型	助记符	说明
1	A	由域名获得IPv4地址
2	NS	查询域名服务器
5	CNAME	查询规范名称
6	SOA	开始授权
11	WKS	熟知服务
12	PTR	把IP地址转换成域名
13	HINFO	主机信息
15	MX	邮件交换
28	AAAA	由域名获得IPv6地址
252	AXFR	传送整个区的请求
255	ANY	对所有记录的请求

- 查询类：通常为1，表明是Internet数据

（2）资源记录(RR)区域

包括回答区域，授权区域和附加区域，格式完全一样。



- 域名：格式和Queries区域的查询名字字段是一样。
- 查询类型：表明资源纪录的类型，与前表一样
- 查询类：对于Internet信息，总是IN
- 生存时间（TTL）

秒为单位，表示资源记录的生命周期，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。

- 资源数据

可变长字段，是按照查询要求返回的相关资源记录数据。可以是Address（表明查询报文想要的回应是一个IP地址）或者CNAME（表明查询报文想要的回应是一个规范主机名）等。

7.2.4 UDP还是TCP

DNS使用的传输层承载协议既可以是UDP也可以是TCP，且端口号均为53.

在大部分情况下，DNS采用UDP协议。但是，当遇到以下情况时，采用TCP：

1.DNS响应报文过长

当名字解析器发出一个查询请求，并且返回响应中的 TC（删减标志）比特被设置为 1时， 即意味着响应的长度超过了512个字节，而仅返回前512个字节。在遇到这种情况时，名字解析器通常使用TCP重发原来的查询请求，允许返回的响应超过512个字节的结果。

2.DNS响应报文过长

在同时拥有主域名（名字）服务器和辅助域名服务器时，辅助服务器将定时（通常是 3小时）向主服务器进行查询以便了解主服务器数据是 否发生变动。

如果有变动，执行一次区域传送。区域传送使用TCP，因为这里传送的数 据远比一个查询或响应多得多。

由于DNS主要使用UDP，而且查询和响应通常经过广域网，分组丢失率和往返时间的不确定性很难控制。因此，在DNS客户端程序中，处理好重传和超时程序就显得十分重要。

7.3 电子邮件协议

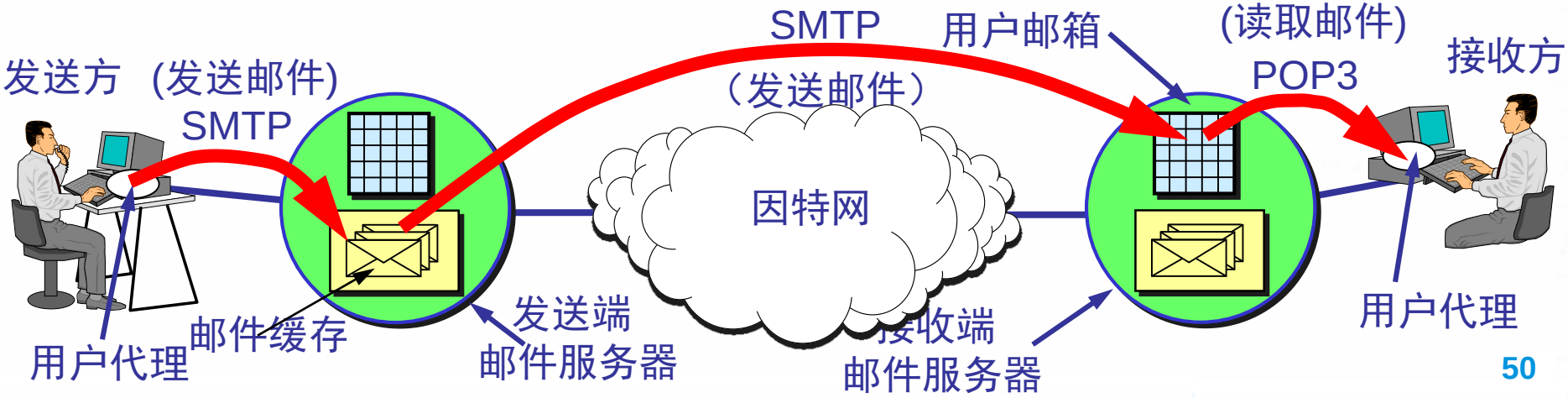
- 电子邮件(e-mail)是因特网上使用得最多的和最受用户欢迎的一种应用。
- 电子邮件把邮件发送到收件人使用的邮件服务器，并放在其中的收件人邮箱中，收件人可随时上网到自己使用的邮件服务器进行读取。
- 电子邮件不仅使用方便，而且还具有传递迅速和费用低廉的优点。
- 现在电子邮件不仅可传送文字信息，而且还可附上声音和图像。

7.3.1 概述

1. 电子邮件的一些标准

- 发送邮件的协议：SMTP
- 读取邮件的协议：POP3 和 IMAP
- MIME 在其邮件首部中说明了邮件的数据类型(如文本、声音、图像、视像等)，使用 MIME 可在邮件中同时传送多种类型的数据。

2. 电子邮件系统的主要组成



（1）用户代理 UA (User Agent)

- 用户代理 UA 就是用户与电子邮件系统的接口，是电子邮件客户端软件。
- 用户代理的功能：撰写、显示、处理和通信。
- 邮件服务器的功能是发送和接收邮件，同时还要向发信人报告邮件传送的情况（已交付、被拒绝、丢失等）。
- 邮件服务器按照客户服务器方式工作。邮件服务器需要使用发送和读取两个不同的协议。

（2）发送和接收电子邮件的步骤

- 发件人调用主机中的用户代理撰写和编辑要发送的邮件。
- 用户代理通过SMTP协议把邮件发给发送方邮件服务器，并暂存在发送邮件服务器的缓存队列中，等待发送。
- 发送方邮件服务器的SMTP客户与接收方邮件服务器的SMTP服务器建立TCP连接，并发送暂存的邮件。
- 接收方邮件服务器中的SMTP服务器进程收到邮件后，把邮件放入收件人的用户邮箱中，等待收件人进行读取。
- 收件人调用主机中的用户代理，使用 POP3（或 IMAP）协议读取发送给自己的邮件。

（3）电子邮件的组成

- 电子邮件由信封(envelope)和内容(content)两部分组成。
- 电子邮件的传输程序根据邮件信封上的信息来传送邮件。用户在从自己的邮箱中读取邮件时才能见到邮件的内容。
- 在邮件的信封上，最重要的就是收件人的地址。

（4）电子邮件地址的格式

TCP/IP 体系的电子邮件系统规定电子邮件地址的格式如下：

收件人邮箱名@邮箱所在主机的域名

- **域名在全世界必须唯一、用户名在该域名的范围内唯一**

7.3.2 简单邮件传输协议

1. 简单邮件传送协议（Simple Mail Transfer Protocol，SMTP）

- SMTP 所规定的就是在两个相互通信的 SMTP 进程之间应如何交换信息。
- 由于 SMTP 使用客户服务器方式，因此负责发送邮件的 SMTP 进程就是 SMTP 客户，而负责接收邮件的 SMTP 进程就是 SMTP 服务器。
- SMTP 规定了 16 条命令和 23 种应答信息；每一种应答信息一般只有一行信息，由一个 3 位数字的代码开始，后面附上（也可不附上）很简单的文字说明。

例如：

MAIL FROM：标识邮件的发件人

RCPT TO：标识邮件的收件人

DATA：启动邮件内容传输

……

220 <domain> Service ready

504 Command parameter not implemented

……

2.电子邮件的信息格式

- 一个电子邮件分为信封和内容两大部分。
- RFC 822 只规定了邮件内容中的首部(header)格式，而对邮件的主体(body)部分则让用户自由撰写。
- 用户写好首部后，邮件系统将自动地将信封所需的信息提取出来并写在信封上。所以用户不需要填写电子邮件信封上的信息。
- 邮件内容首部包括一些关键字，后面加上冒号。最重要的关键字是：To 和 Subject。

3. 邮件内容的首部

- “To:”后面填入一个或多个收件人的电子邮件地址。用户只需打开地址簿，点击收件人名字，收件人的电子邮件地址就会自动地填入到合适的位置上。
- “Subject:”是邮件的主题。它反映了邮件的主要内容，便于用户查找邮件。
- 抄送 “Cc:” 表示应给某某人发送一个邮件副本。
- “From” 和 “Date” 表示发信人的电子邮件地址和发信日期。“Reply-To” 是对方回信所用的地址。

7.3.3 邮件读取协议

1. POP3协议

POP3是Post Office Protocol 版本3的简称，是TCP/IP协议簇中的一员（默认端口是110）。POP3协议主要用于支持使用客户端远程管理在服务器上的电子邮件。POP3规定怎样将主机连接到Internet的邮件服务器和下载电子邮件的电子协议。

- 邮局协议 POP 是一个非常简单、但功能有限的邮件读取协议，现在使用的是它的第三个版本 POP3。
- POP 也使用客户服务器的工作方式。
- 在接收邮件的用户 PC 机中必须运行 POP 客户程序，而在用户所连接的 ISP 的邮件服务器中则运行POP 服务器程序。

2. IMAP 协议

Internet邮件访问协议（Internet Mail Access Protocol，IMAP），以前称为交互式邮件访问协议（Interactive Mail Access Protocol）。

IMAP协议运行在TCP/IP协议之上，使用TCP协议，端口号为143。IMAP也是一种用于接收邮件的协议，与POP3协议的主要区别是用户可以不用把所有的邮件全部下载，可以通过客户端直接对服务器上的邮件进行操作。

- IMAP 也是按客户服务器方式工作，现在较新的是版本4，即 IMAP4。
- 用户在自己的 PC 机上就可以操纵 ISP 的邮件服务器的邮箱，就像在本地操纵一样。
- 因此 IMAP 是一个联机协议。当用户 PC 机上的 IMAP 客户程序打开 IMAP 服务器的邮箱时，用户就可看到邮件的首部。若用户需要打开某个邮件，则该邮件才传到用户的计算机上。

IMAP 的特点

- IMAP最大的好处就是用户可以在不同的地方使用不同的计算机随时上网阅读和处理自己的邮件。
- IMAP 还允许收件人只读取邮件中的某一个部分。例如，收到了一个带有视像附件（此文件可能很大）的邮件。为了节省时间，可以先下载邮件的正文部分，待以后有时间再读取或下载这个很长的附件。
- IMAP 的缺点是如果用户没有将邮件复制到自己的 PC 机上，则邮件一直是存放在 IMAP 服务器上。因此用户需要经常与 IMAP 服务器建立连接。

（3）必须注意

- 不要将邮件读取协议 POP 或 IMAP 与邮件传送协议 SMTP 弄混。
- 发信人的用户代理向源邮件服务器发送邮件，以及源邮件服务器向目的邮件服务器发送邮件，都是使用 SMTP 协议。
- 而 POP 协议或 IMAP 协议则是用户从目的邮件服务器上读取邮件所使用的协议。

本章作业

1.应用层协议的体系架构有哪几种模式？各有什么特点？

2.根据应用领域的特点，应用层协议可能会对传输层协议提出哪几种要求？TCP/IP能够实现哪些要求？

3.什么是域名、域名结构和绝对域名？

4.阐述DNS的工作原理和解析过程。

5.结合DNS的报文结构，说明DNS在什么情况下使用UDP协议？什么情况下使用TCP协议？为什么？

6.在电子邮件中，有哪几种主要协议？分别有什么作用？