计算机网络

Computer Network

13

域名系统

理论课程

厦門大學

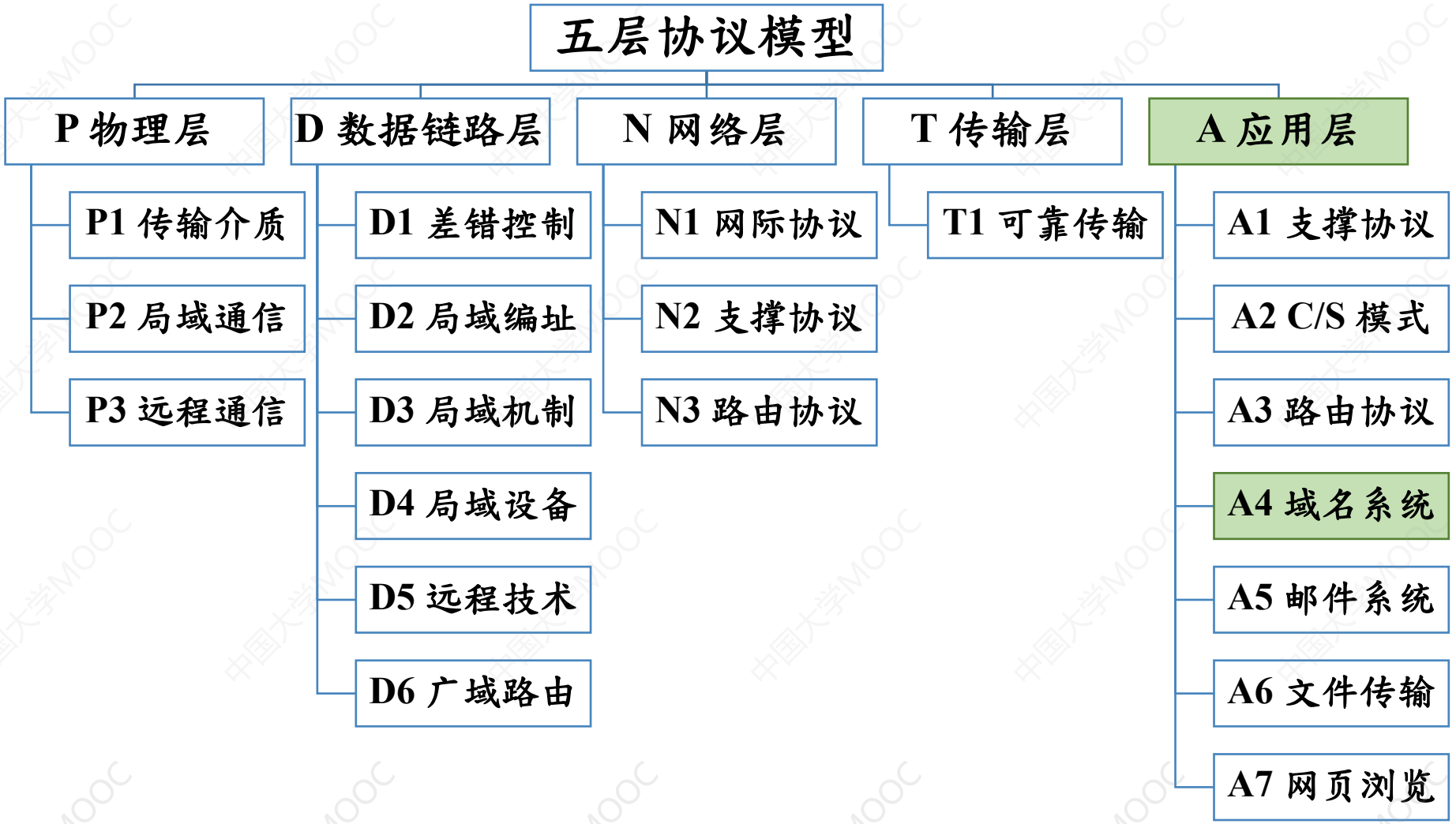
XIAMEN UNIVERSITY

信息学院 黄 炜

(特色化示范性软件学院) 博士,副教授

School of Informatics Wei Huang

知识框架


五层协议模型
P 物理层
D 数据链路层
N 网络层
T 传输层
A 应用层
P1 传输介质
P2 局域通信
P3 远程通信
D1 差错控制
D2 局域编址
D3 局域机制
D4 局域设备
D5 远程技术
D6 广域路由
N1 网际协议
N2 支撑协议
N3 路由协议
T1 可靠传输
A1 支撑协议
A2 C/S 模式
A3 路由协议
A4 域名系统
A5 邮件系统
A6 文件传输
A7 网页浏览

主要内容

- 域名、域名分级
- 域名服务器分级
- 域名服务（DNS）
  - 递归、迭代的工作原理

对应课本章节

- **PART I Introduction And Internet Applications**
  - **Chapter 4 Traditional Internet Applications**
    - **4.17~4.26 Domain Name System (DNS); Domain Names That Begin With www; The DNS Hierarchy And Server Model; Name Resolution; Caching In DNS Servers; Types Of DNS Entries; Aliases And CNAME Resource Records; Abbreviations And The DNS; Internationalized Domain Names**

内容纲要

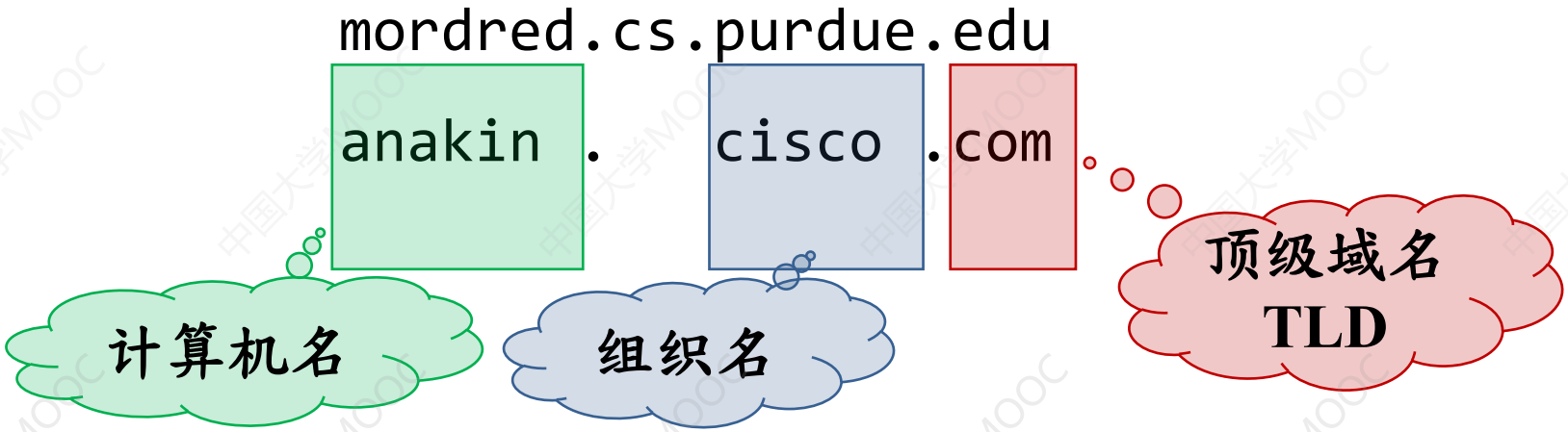
1. 域名结构
2. 域名服务器的模型
3. 域名解析过程
4. 选作作业

域名系统

- 域名系统（Domain Name System， DNS ）
  - 提供了将人类可读符号域名映射到计算机地址的服务
    - 注意：计算机地址不只是IP地址
- 分布式
  - 名字到 IP 地址的解析由若干个域名服务器程序完成。
  - 域名服务器程序在专设的结点上运行，运行该程序的机器称为域名服务器。

域名结构

- 域名
  - 因特网上的主机或路由器所具有的唯一的层次结构的名字。
- 层次树状结构
  - 域名的结构由标号序列组成，各标号之间用点隔开：
    - 与IP地址的点完全不同



域名与IP地址的区别

- 域名只是个逻辑概念，并不代表计算机所在物理地点。
- 域名和IP地址的区别
  - 变长的域名和使用有助记忆的字符串，是为了便于人使用。
  - IP 地址是定长的 32 位数字则非常便于机器进行处理。

顶级域名 (Top Level Domain, TLD)

- 国家或地区顶级域名
- 通用顶级域名
- 基础结构域名： arpa

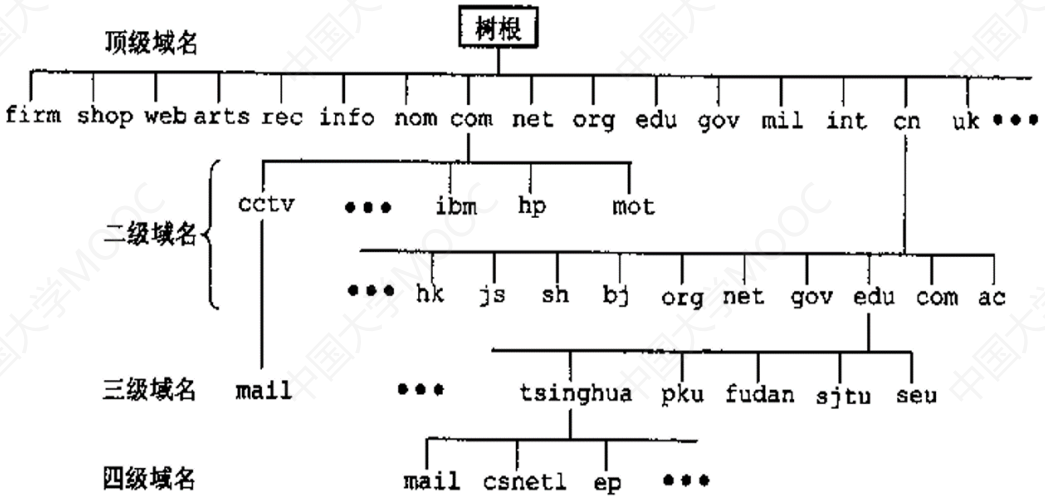


图 12-1 因特网的名字空间

Domain Name	Assigned To
aero	Air transport industry
arpa	Infrastructure domain
asia	For or about Asia
biz	Businesses
com	Commercial organizations
coop	Cooperative associations
edu	Educational institutions
gov	United States Government
info	Information
int	International treaty organizations
jobs	Human resource managers
mil	United States military
mobi	Mobile content providers
museum	Museums
name	Individuals
net	Major network support centers
org	Non-commercial organizations
pro	Credentialed professionals
travel	Travel and tourism
country code	A sovereign nation

域名区

- 区（zone）
  - 一个服务器所负责管辖的（或有权限的）范围。
  - 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”（domain）为单位，而是以“区”为单位。

域名别名

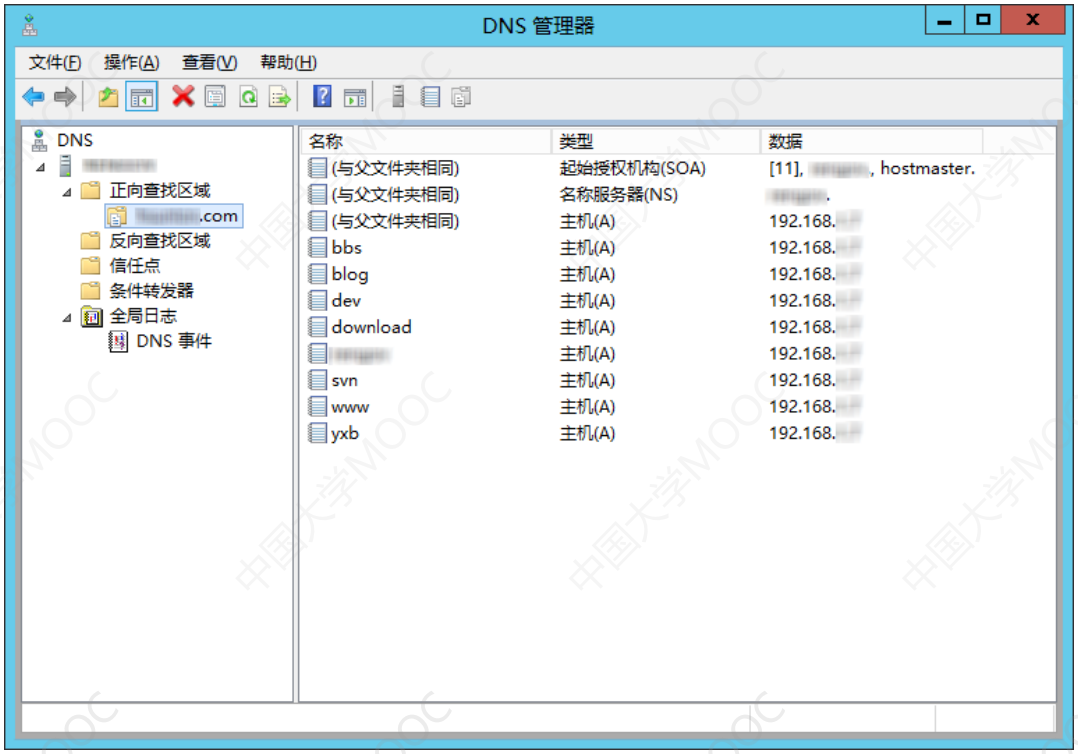
- 许多组织指定反映计算机提供服务的域名

```
ftp.foobar.com
www.foobar.com
```

  - 助记符，但不需要
- 使用www来命名运行Web服务器的计算机是一个惯例
  - 任意计算机可以运行Web服务器，即使域名不包含www
  - 一个具有www域名的计算机不需要运行Web服务器

DNS层次结构和服务器模型

- 每个组织可以自由选择其服务器的详细信息
  - 将组织所有域名放置在单个物理服务器或多台服务器之间



内容纲要

1. 域名结构
2. 域名服务器的模型
3. 域名解析过程
4. 选作作业

域名服务器的四种类型

- 根域名服务器
  - 存储所有顶级域名服务器的地址信息。
- 顶级域名服务器
  - 保存顶级域名下一级区的权限域名服务器。
- 权限域名服务器
  - 保存该区中的所有主机的域名到IP地址的映射。
- 本地域名服务器
  - 进行具体主机的域名解析服务。

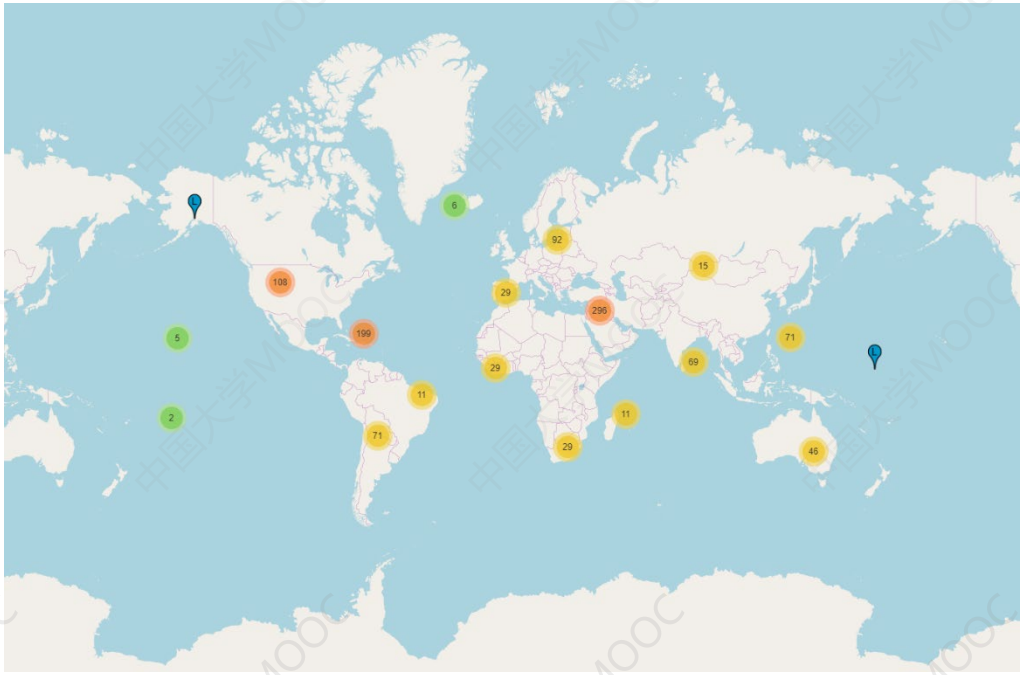
根域名服务器

- 根域名服务器是最重要的域名服务器。
  - 根域名服务器知道所有顶级域名服务器的域名和 IP 地址。
  - 本地域名服务器，只要自己无法解析某个域名，就首先求助于根域名服务器。

根域名服务器

- 因特网逻辑上有 13 个不同 IP 地址的根域名服务器
  - 名字用一个英文字母命名，从 a 一直到 m（前 13 个字母）。
  - 世界已有900多个根域名服务器

```
a.root-servers.net
b.root-servers.net
…
m.root-servers.net
```



顶级域名服务器

- 顶级域名服务器
  - 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

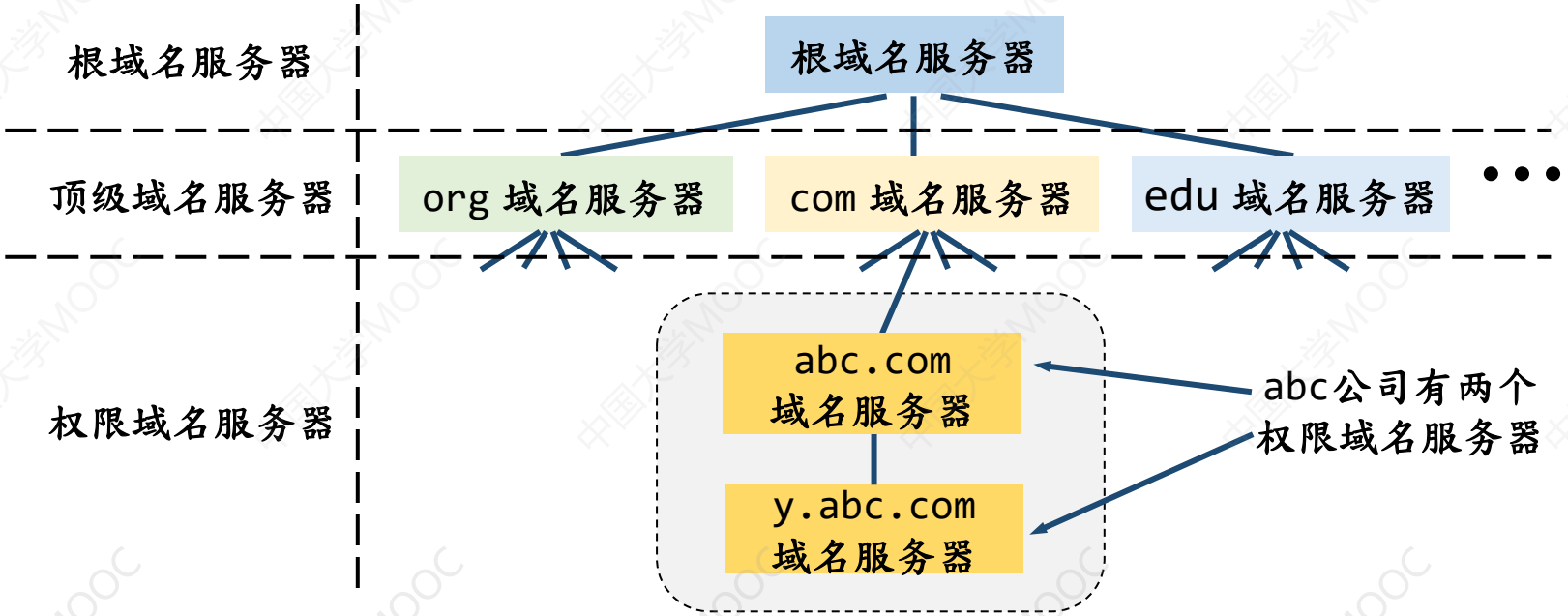
- 权限域名服务器
  - 负责一个区的域名服务器。
- 作用
  - 当一个权限域名服务器还不能给出最后的查询回答时，就会告诉发出查询请求的 DNS 客户，下一步应当找哪一个权限域名服务器。

本地域名服务器

- 本地域名服务器（默认域名服务器）
  - 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，
- 本地服务器对域名系统非常重要。

本地域名服务器和根域名服务器

- 每台主机应知道本地域名服务器（ local name server ）
  - 一般是通过网卡属性获得信息并手工配置
- 每台LNS应知道根域名服务器（ root name servers ）



提高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。

内容纲要

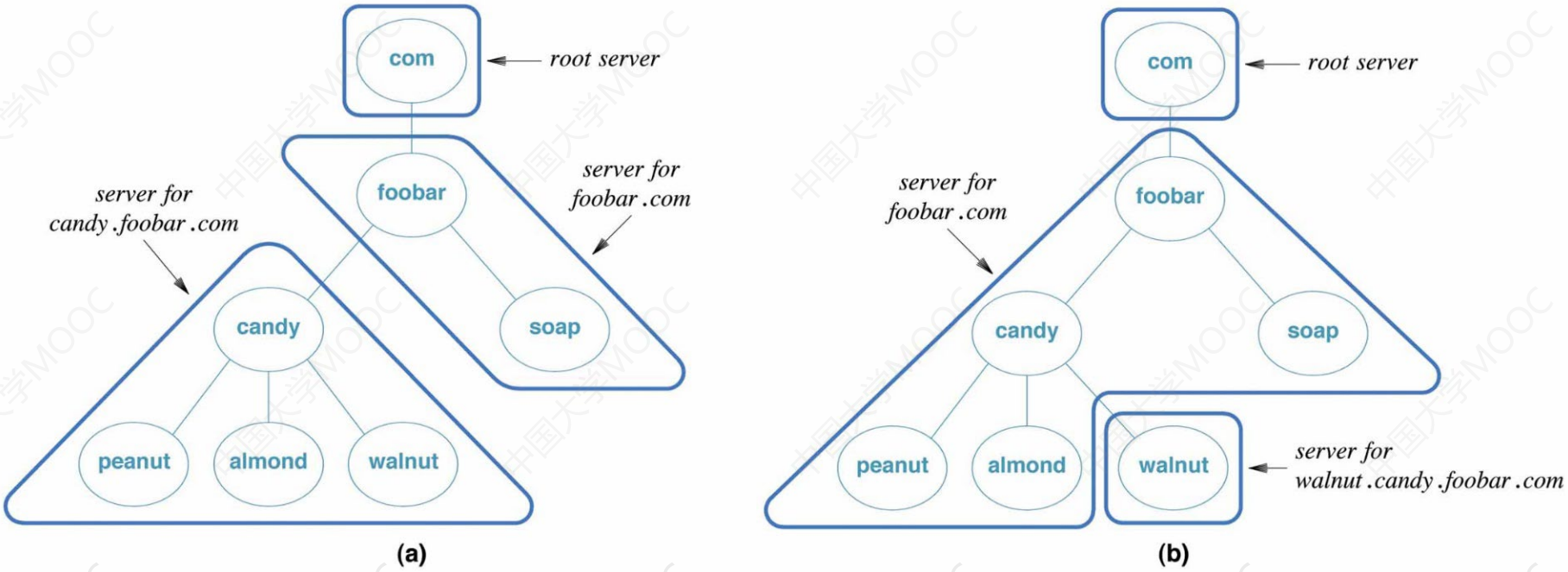
1	域名结构
2	域名服务器的模型
3	域名解析过程
4	选作作业

域名的解析过程

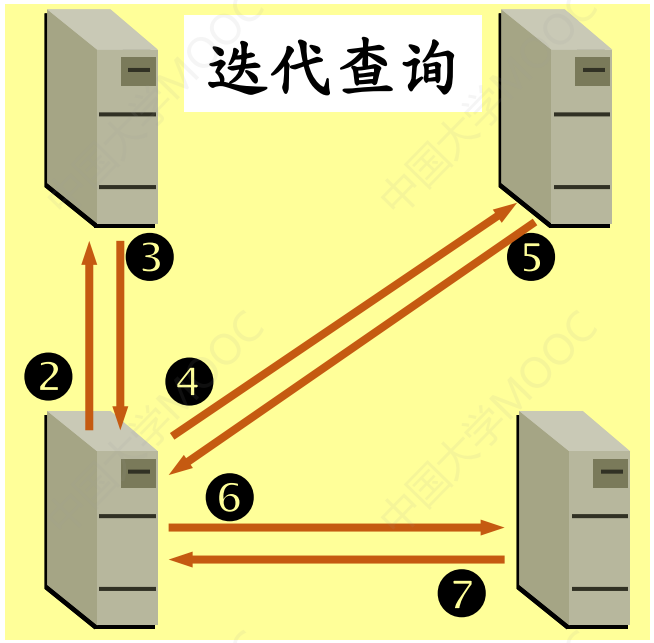
- 递归查询：主机向本地域名服务器的查询。
  - 如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文。
- 迭代查询：本地域名服务器向根域名服务器的查询。
  - 当根域名服务器收到本地域名服务器的迭代查询请求报文，要么给出所查询 IP 地址，要么告诉本地域名服务器下一步应向服务器查询，然后让本地域名服务器进行后续查询。

层次结构和服务器模型

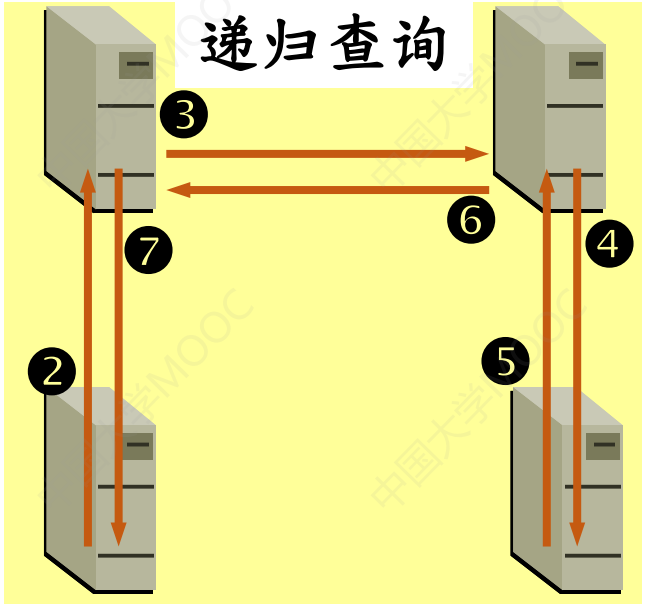
- 允许每个组织将域名分配到计算机或更改这些域名而不通知中央管理局



本地域名服务器迭代查询



本地域名服务器递归查询（较少用）



域名高速缓存

- 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，并处理超时的项。
  - 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。

域名解析

- 域名解析（name resolution）
  - 域名翻译成一个地址被称为域名解析
  - 执行的软件称为域名解析器（或解析器，resolver）
  - Socket API： `gethostbyname`
  - 解析器通过连接DNS服务器成为客户端
  - DNS服务器返回对调用者的回答
- 使用流（stream）模式或消息（message）模式

DNS条目类型

- DNS数据库中的每个条目由三个项目组成
  - 一个域名，一个记录类型（ record type ）和一个值
- 发送到DNS服务器的查询指定域的域名和类型，服务器只返回与查询类型相匹配的绑定
- 主要的类型将域名映射到IP地址
  - DNS将此绑定分类为类型A：用于应用程序
  - DNS支持几个其他类型，包括类型MX，指定邮件交换器
  - 返回的地址取决于类型

资源记录

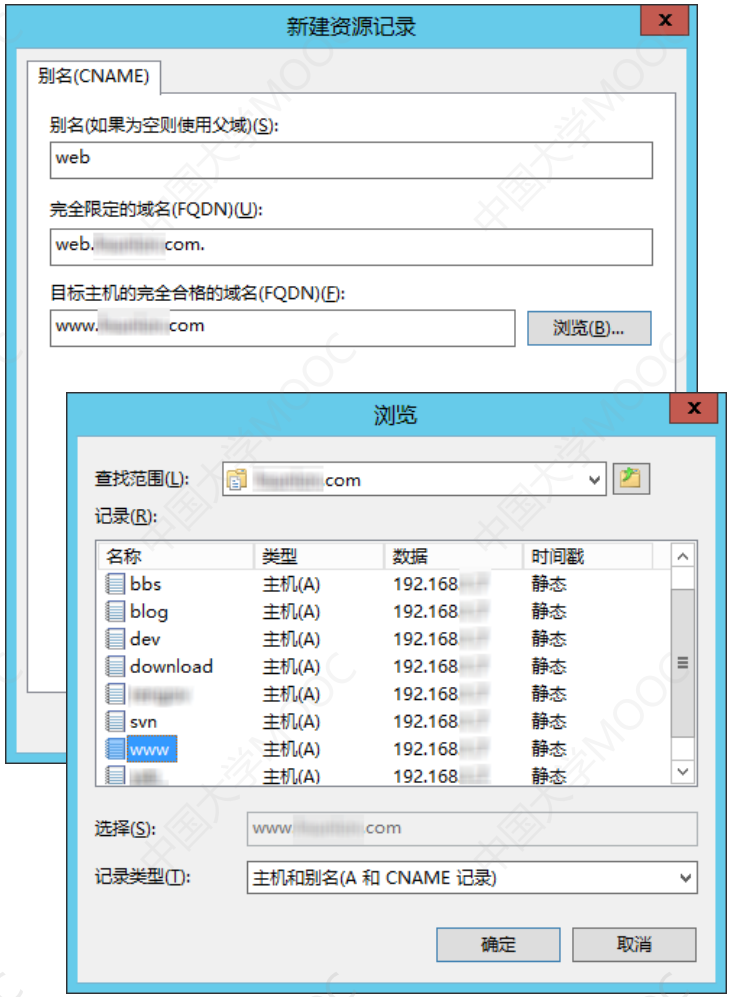
- 每个服务器用资源记录（Resource Record）的集合实现区域信息。本质上，资源记录是名字到值的绑定
  - <名字Name, 值Value, 类型Type, 分类Class, 生存期TTL>
- 名字name/值value：主机名字到IP地址
- 分类Class
  - 允许其他实体（除InterNIC外）定义有用的记录类型，目前广泛使用的分类是因特网使用的分类，记IN。
- 生存期TTL：指明资源记录的有效期限

资源记录中各个字段的含义

- 类型type
  - NS：值字段给出了运行名字服务器的主机域名，而该名字服务器知道如何解析特定的域名
  - CNAME：值字段给出了特定主机的规范名字，主要用于定义主机别名
  - MX：值字段给出了运行邮件服务器的主机域名，而该邮件服务器知道如何接收解析指定域的值

别名和CNAME资源记录

- DNS提供了一个CNAME
  - 为另一个DNS条目提供别名很有用
- 假设foobar.com下有名为abc的计算机，运行一段时间后，希望将其部署为Web服务器。
  - 最好以www.foobar.com为域名
  - CNAME可不必重复部署或改名



国际化域名

- DNS使用ASCII 字符集
- 国际化域名应用（IDNA）
  - 因特网工程工作组(http://www.ietf.org)在RFC 3490下定义的一个协议
- 中文域名

内容纲要

1	域名结构
2	域名服务器的模型
3	域名解析过程
4	选作作业

选作作业

- 用Wireshark监听收发DNS的数据流
  - 访问厦门大学信息学院软件工程系主页
  - 浏览器对DNS的访问是基于TCP的还是UDP的
- 请你的同学配合，在不同地方ping一些门户网站的主机，查看DNS是否指向同一个IP地址，这样做有何好处？（是不是意味着访问不同的内容？）

计 算 机 网 络

Computer Network

13

谢谢观看

理论课程

厦門大學

XIAMEN UNIVERSITY

信息学院 黄 煒

(特色化示范性软件学院) 博士,副教授

School of Informatics Wei Huang