- 网络计算模式
  - 概述
  - 企业计算
  - 网格计算和云计算
  - P2P网络、CDN网络和物联网
  - 社会计算

域名系统

主要内容

- 互联网的命名机制
- 域名服务器、域名解析器与域名解析算法
- 提高域名解析效率的基本方法
- DNS记录
- DNS协议

域名系统

为什么要使用域名?

✦问题的提出：TCP/IP互联网中，可以使用IP地址标示主机对一般用户而言，IP地址非常抽象，不是十分直观，用户希望利用好读、易记的字符串来标示主机。

✦域名系统希望解决的主要问题：主机名的管理，主机名—IP地址映射等。

域名系统

互联网命名机制应解决的3个问题?

- ✦全局惟一性：一个特定的主机名在整个互联网上是惟一的
- ✦名字便于管理：分配名字、确认名字、回收名字
- ✦高效地进行映射：高效地将主机名映射为IP地址（或将IP地址映射为主机名）

域名系统

互联网命名机制的分类

- 无层次命名机制
- 层次型命名机制

域名系统

☙无层次命名机制

✦无层次命名机制的概念：主机的名字简单地由一个字符串组成，该字符串没有进一步的结构。

✦特点：名字的分配、确认、以及回收等工作可以由一个部门集中管理；名字-地址之间的映射可以通过一对一的表格实现。

✦缺点：随着互联网中主机的大量增加，名字冲突的可能性越来越大，单一管理机构的工作负担越来越大。无论是在每一网点维护一个名字-地址映射表拷贝，还是采用集中式单一映射表都是低效的。

无层次命名机制已被TCP/IP互联网淘汰

域名系统

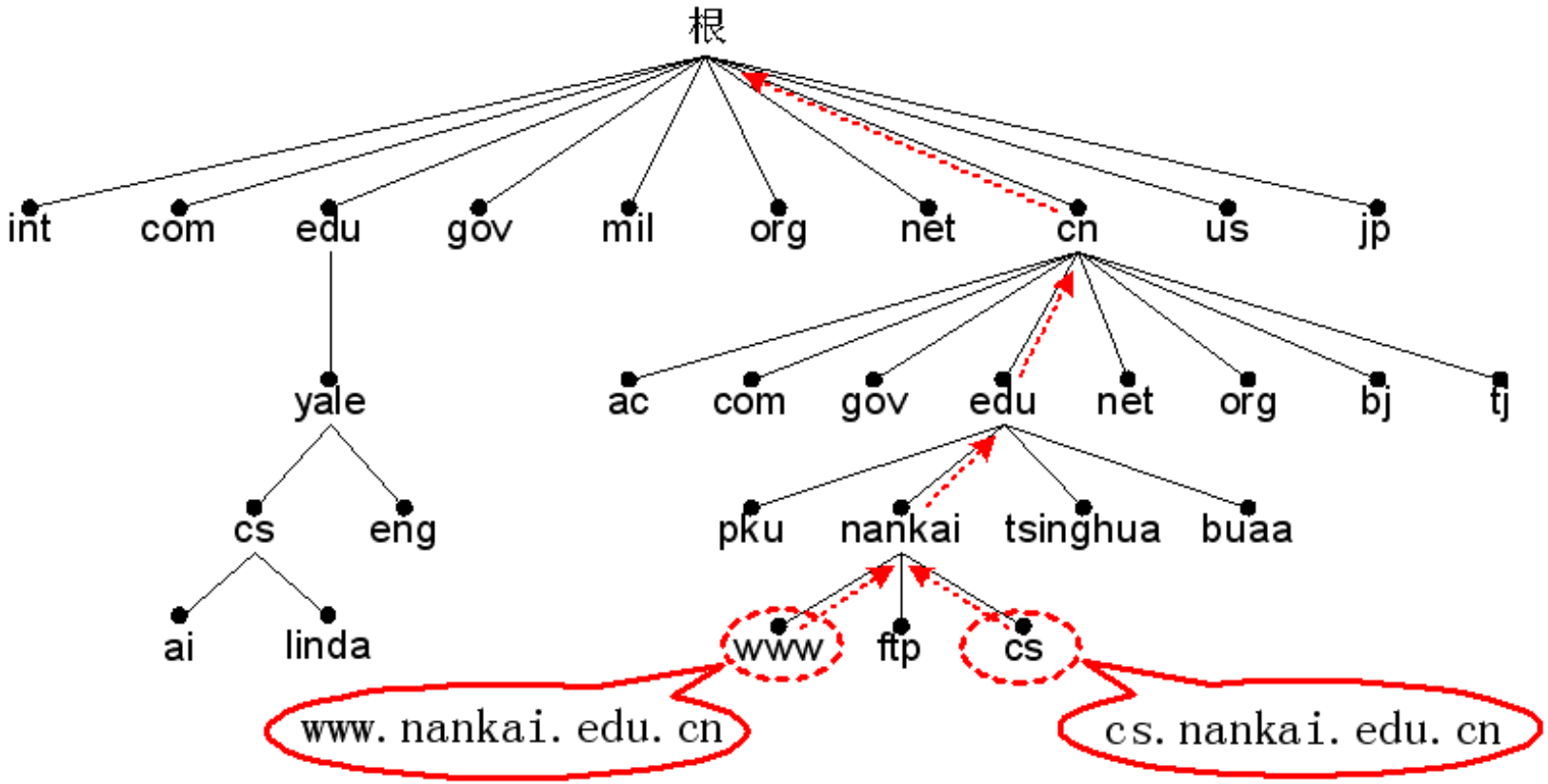
☙层次型命名机制

✦层次型命名机制的概念：在名字中加入结构，而这种结构是层次型的。

✦层次型名字的树状结构：树中的每一节点都有一个相应的标识符；主机名就是从树叶到树根（或从树根到树叶）路径上各节点标识符的有序序列。

域名系统

☙层次型命名机制



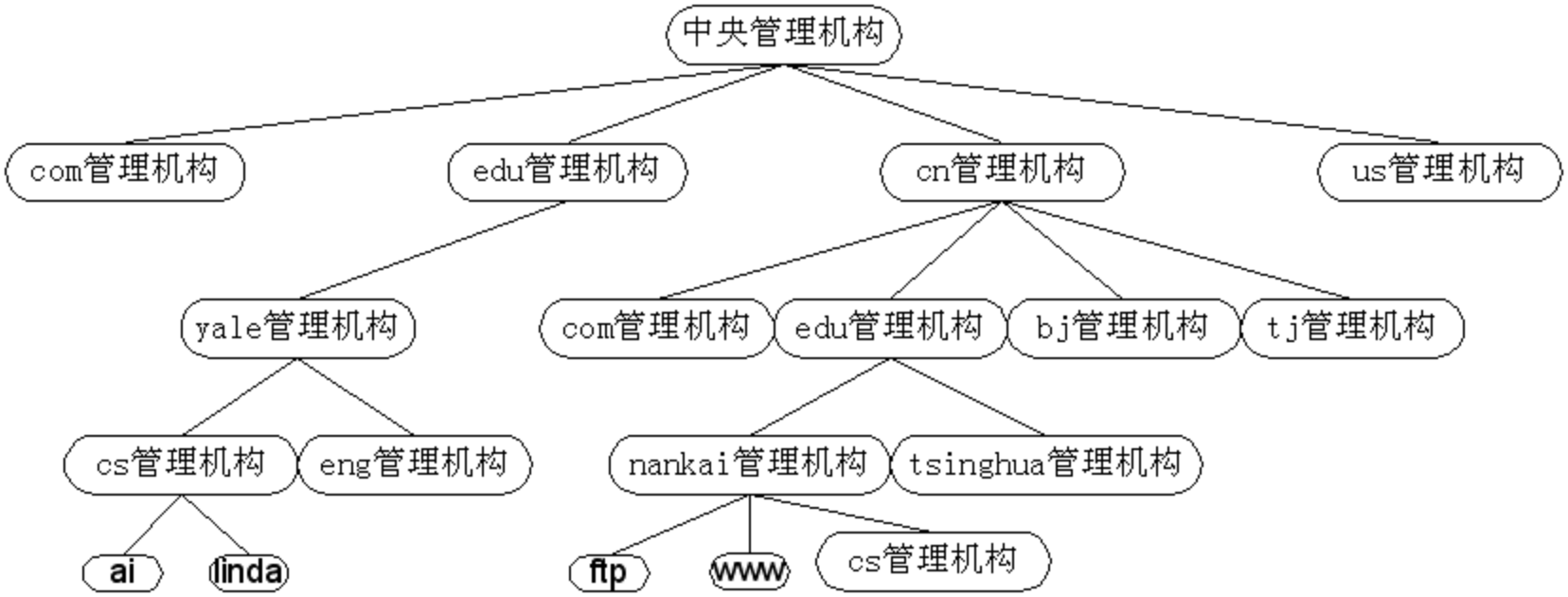
域名系统

☙层次型命名机制的特点

- ✦只要同一子树下每层节点的标识符不冲突，完整的主机名绝对不会冲突。
- ✦层次型命名机制有利于层次型的名字管理。
- ✦层次型命名机制有利于高效地进行名字-地址的映射（详见域名解析部分）。

域名系统

☙层次型命名机制



域名系统

TCP/IP互联网域名

1.域名系统

TCP/IP互联网中实现的层次型名字管理机制

2.域名系统规定的主要内容

名字语法以及名字管理特权的分派规则

名字-地址映射分布式计算机系统的实现方法

3. 域名系统的命名机制

完整的域名由名字树中的一个节点到根节点路径上节点标识符的有序序列组成，其中节点标识符之间以“.”隔开

标号：节点标识符被称为标号

域：由每一标号后面的各标号组成

域名系统

TCP/IP互联网域名与Internet域名

1.TCP/IP互联网域名

是一种抽象的标准

各标号值可任意填写

任何组织均可根据域名语法构造本组织内部的域名

2.Internet域名

因特网是一个国际性的大型互联网

因特网规定了一组正式的通用标准标号

域名系统

Internet顶级域名的划分

顶级域名	分配给
com	商业组织
edu	教育机构
gov	政府部门
mil	军事部门
net	主要网络支持中心
org	上述以外的组织
int	国际组织
国家代码	各个国家

域名系统

Internet中国二级域名分配举例

划分模式	二级域名	分配给
类别域名（6 个）	ac	科研机构
	com	工、商、金融等企业
	edu	教育机构
	gov	政府部门
	net	互联网络、接入网络的信息中心和运行中心
	org	各种非盈利性的组织
行政区域名（34 个）	bj	北京市
	sh	上海市
	tj	天津市
	cq	重庆市
	he	河北省
	sx	山西省
	nm	内蒙古自治区
	……	……

域名系统

域名解析

1.为什么要进行域名解析?

用户希望使用记忆和书写较为方便的域名

主机之间的通信仍然需要通过IP地址进行

必须提供一种机制进行域名与IP地址之间的映射

2.什么是域名解析?

将域名映射为对应的IP地址（或将IP地址映射为对应的域名）

域名解析需要借助于一组既相互独立又相互协作的域名服务器完成

域名系统

☙域名服务器与域名解析器

1.域名服务器

一个服务器软件，运行在指定的主机上，完成域名-IP地址映射

一个域名服务器通常保存着它所管辖区域内的域名与IP地址对照表

2.域名解析器

请求域名解析服务的客户软件

一个域名解析器可以利用一个或多个域名服务器进行域名解析

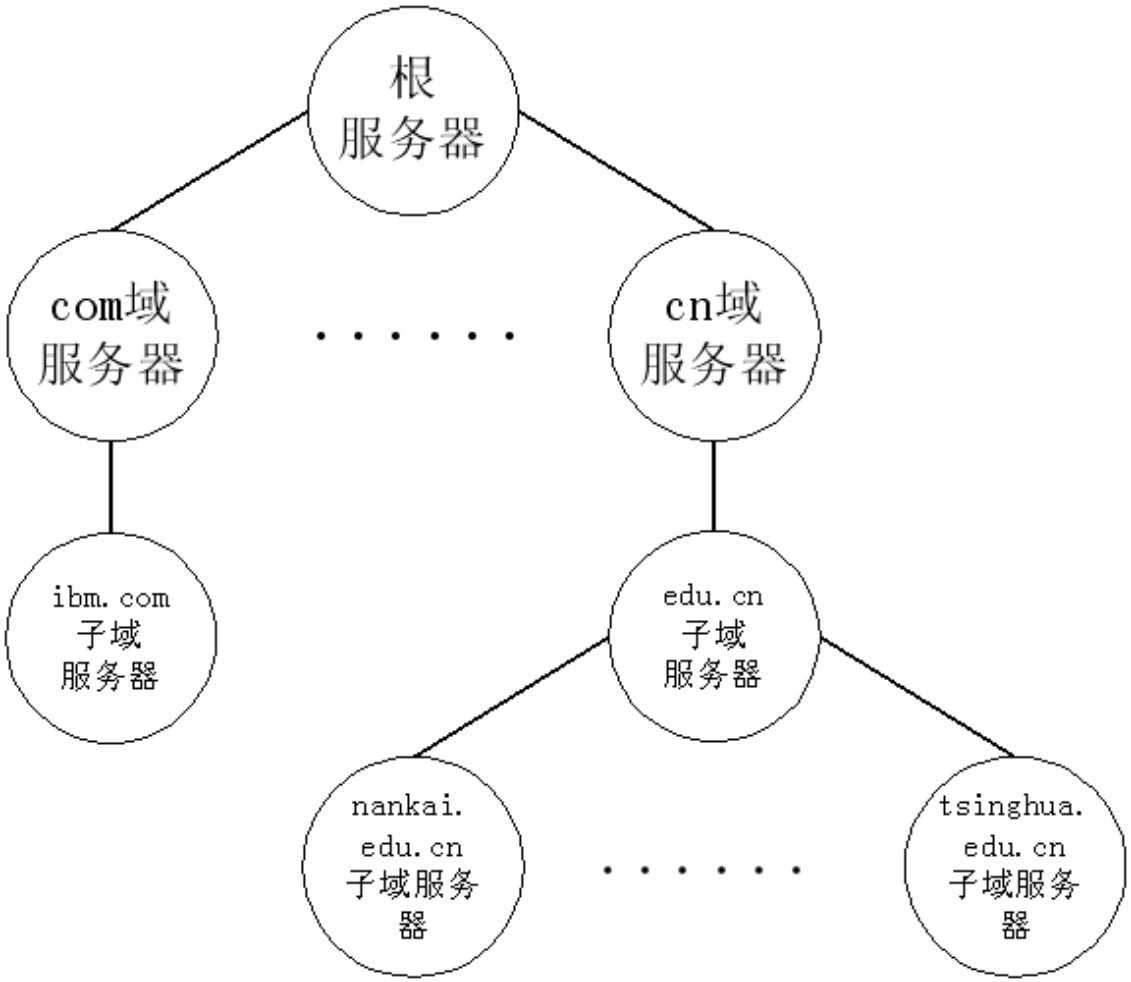
域名系统

域名服务器的层次结构

- ✦树形逻辑结构是域名解析算法赖以实现的基础
- ✦域名解析采用自顶向下的算法
- ✦解析过程只需走过一条从根节点到另一节点的单向路径，无需回溯，更不用遍历整个服务器树
- ✦注意：解析过程都从根服务器开始不是很好的解决方案

域名系统

域名服务器的层次结构



域名系统

☙域名解析需要的已知条件

1.域名解析器

至少知道任意一个域名服务器的IP地址

2.域名服务器

至少知道根服务器的IP地址

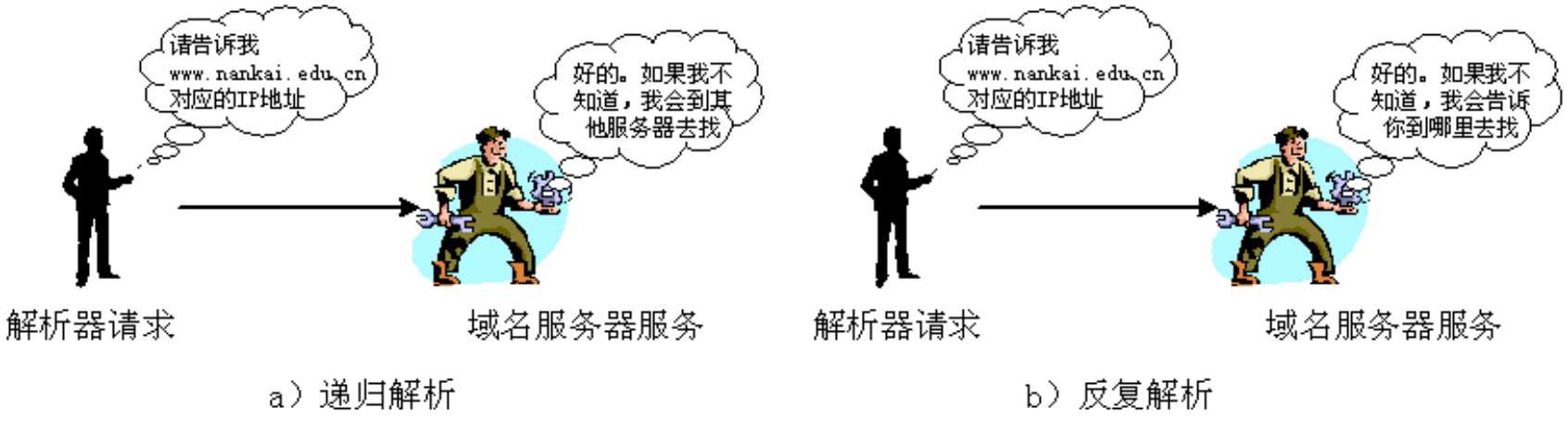
至少知道父节点服务器的IP地址

域名系统

☙域名服务器的解析方式

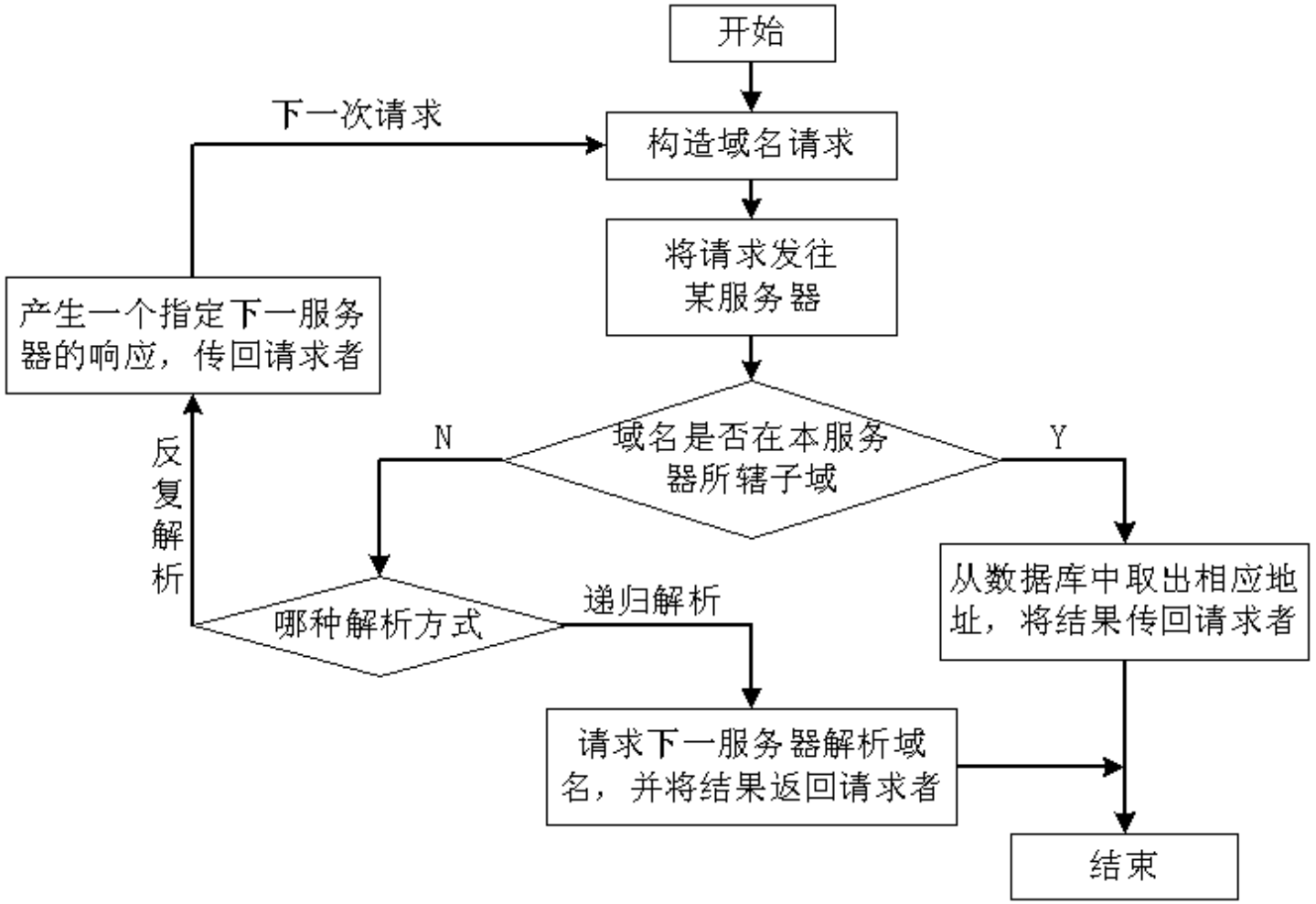
✦递归解析（recursive resolution）：要求域名服务器系统一次性完成全部名字—地址变换

✦反复解析（iterative resolution）：每次请求一个服务器，不行再请求其他的服务器。



域名系统

☙域名服务器的解析流程



域名系统

☙提高域名解析效率

1.解析从本地域名服务器开始

2.域名服务器的高速缓冲技术

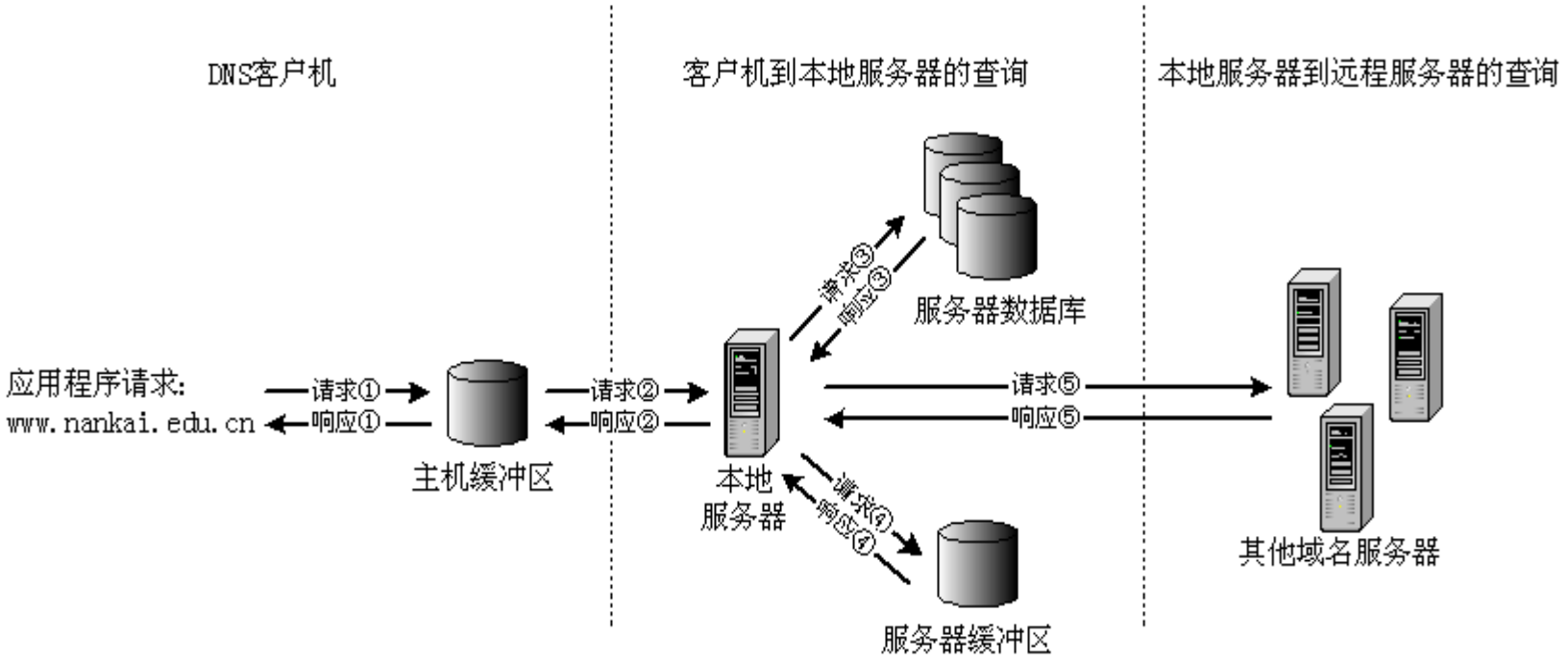
(1)域名服务器将其最近解析过的域名与IP地址的映射关系存放在自己的高速缓冲区中。

(2)保证缓冲区中域名—IP地址映射关系的有效性：向解析器报告缓冲信息时，注明这是“非权威性”映射，并给出获取该映射的域名服务器IP地址； 为缓冲区中每一映射关系设置最大生存周期。

3.主机上的高速缓冲技术

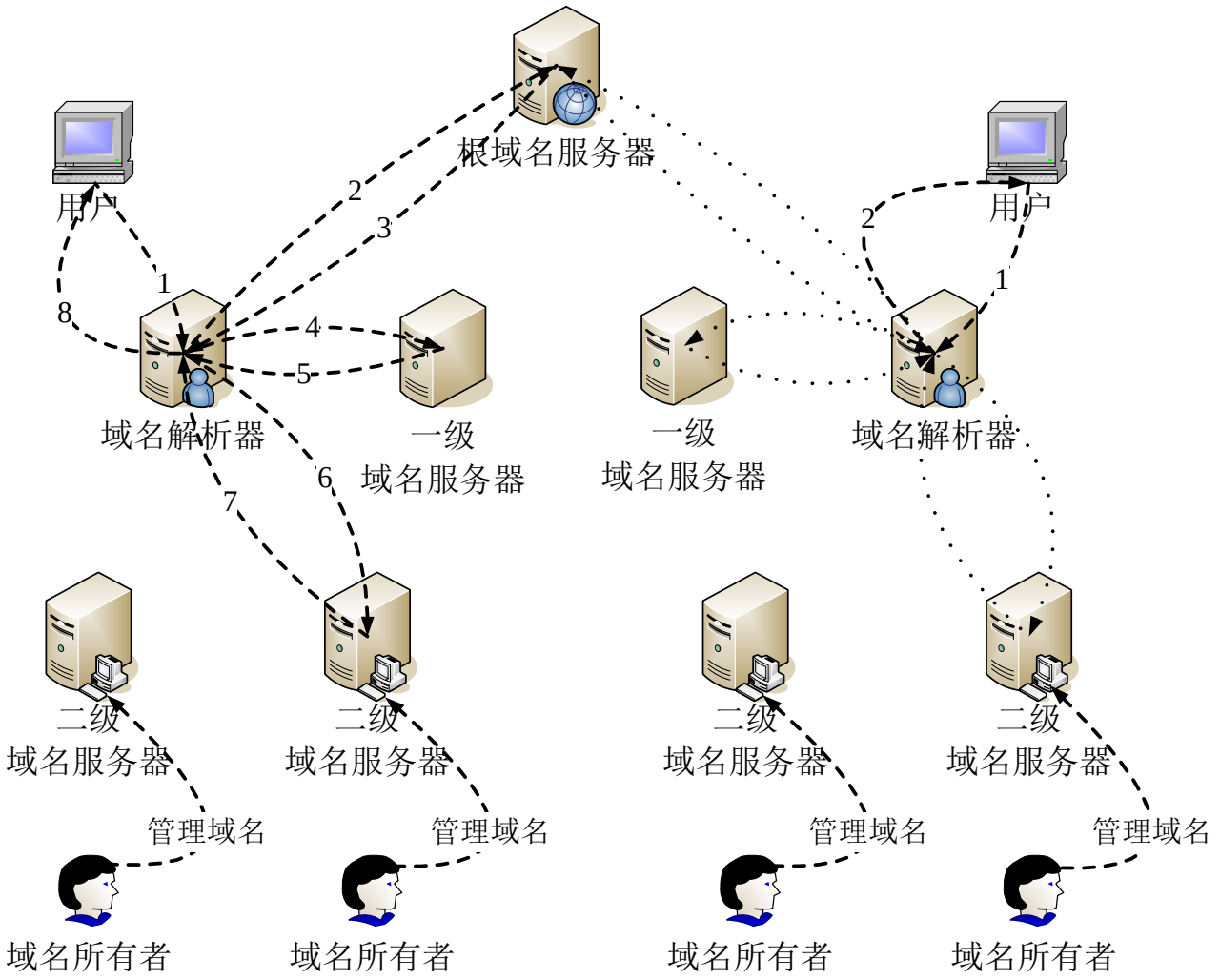
域名系统

域名解析过程


DNS客户机
客户机到本地服务器的查询
本地服务器到远程服务器的查询
应用程序请求:
www.nankai.edu.cn
请求①
响应①
主机缓冲区
请求②
响应②
本地
服务器
请求③
响应③
服务器数据库
请求④
响应④
服务器缓冲区
请求⑤
响应⑤
其他域名服务器

域名系统

域名解析系统架构



域名系统

☙域名解析系统架构

✦域名解析系统架构，采用分布式层级结构的设计，由域名解析器和各级域名服务器构成。每级域名空间有与之对应的域名服务器。各级域名服务器在地理上分散分布，在逻辑上以树形结构展开，依次为根域名服务器（对应根域名）、一级域名服务器（对应顶级域名）、二级域名服务器（对应二级域名）等。

✦从宏观上看，现行域名解析系统可以分为客户端和服务器端两部分。客户端，即域名解析器，负责访问各级域名服务器，缓存**非权威的DNS记录**，响应用户的域名解析请求。服务器端，即域名服务器，通常由域名所有者进行管理和维护，负责维持其对应域名的**权威的DNS记录**。

域名系统

DNS记录

✦在域名服务器的数据库中，每条域名与其IP地址的映射关系等信息都以DNS记录的方式存放。

✦DNS记录通常由域名、有效期、类别、类型和具体值组成。包括A类DNS记录（用于记录域名对应的32比特的IPv4地址）、AAAA类DNS记录（用于记录域名对应的128比特的IPv6地址）、NS类DNS记录（用于指定域名所对应的域名服务器的IP地址）、CNAME类DNS记录（用于指定域名的别名，可将多个域名映射到同一台主机）、MX类DNS记录（用于指定域名的邮件服务器的IP地址）等。

域名系统

DNS记录

类型	意义	内容
SOA	授权开始	标识一个资源记录集合（称为授权区段）的开始
A	主机地址	32 位二进制值 IP 地址
MX	邮件交换机	邮件服务器名及优先级
NS	域名服务器	域的授权名子服务器名
CNAME	别名	别名的规范名字
PTR	指针	对应于 IP 地址的主机名
HINFO	主机描述	ASCII 字符串，CPU 和 OS 描述
TXT	文本	ASCII 字符串，不解释

域名系统

DNS记录

域名	TTL(秒)	类别	类型	值
nankai.eud.cn	86400	IN	SOA	NankaiDNS (……)
nankai.edu.cn	86400	IN	TXT	"Nankai University"
netlab.nankai.eud.cn	86400	IN	HINFO	HP Unix
netlab.nankai.edu.cn	86400	IN	A	202.113.27.53
netlab.nankai.edu.cn	86400	IN	MX	5 mail.netlab.nankai.edu.cn
Mail.netlab.nankai.edu.cn	86400	IN	A	202.113.27.55
Info.netlab.nankai.edu.cn	86400	IN	A	202.113.27.54
www.netlab.nankai.edu.cn	86400	IN	CNAME	info.netlab.Nankai.edu.cn
ftp.netlab.nankai.edu.cn	86400	IN	CNAME	info.netlab.nankai.edu.cn

域名系统

DNS记录

✦**非权威的DNS记录（Non-Authoritative DNS Record）：**非权威的DNS记录是指域名解析器上缓存的DNS记录。域名解析器通过访问域名服务器获取权威的DNS记录后，在将该权威的DNS记录返回给用户的同时，也将缓存该DNS记录。此缓存的DNS记录受限于TTL（Time-to-Live）值，若TTL值超期，域名解析器将不再缓存此DNS记录。在TTL值有效期内，若收到域名解析请求，域名解析器则立即将此DNS记录返回给用户，以提高域名解析效率。但是，在此TTL值有效期内，域名服务器上权威的DNS记录可能发生更新，则此缓存的DNS记录可能成为冗余信息，不具有权威性。

域名系统

DNS记录

✦**权威的DNS记录（Authoritative DNS Record）：**权威的DNS记录是指域名服务器上维持的DNS记录，是由域名所有者或通过其它动态的DNS方法直接管理的DNS记录。

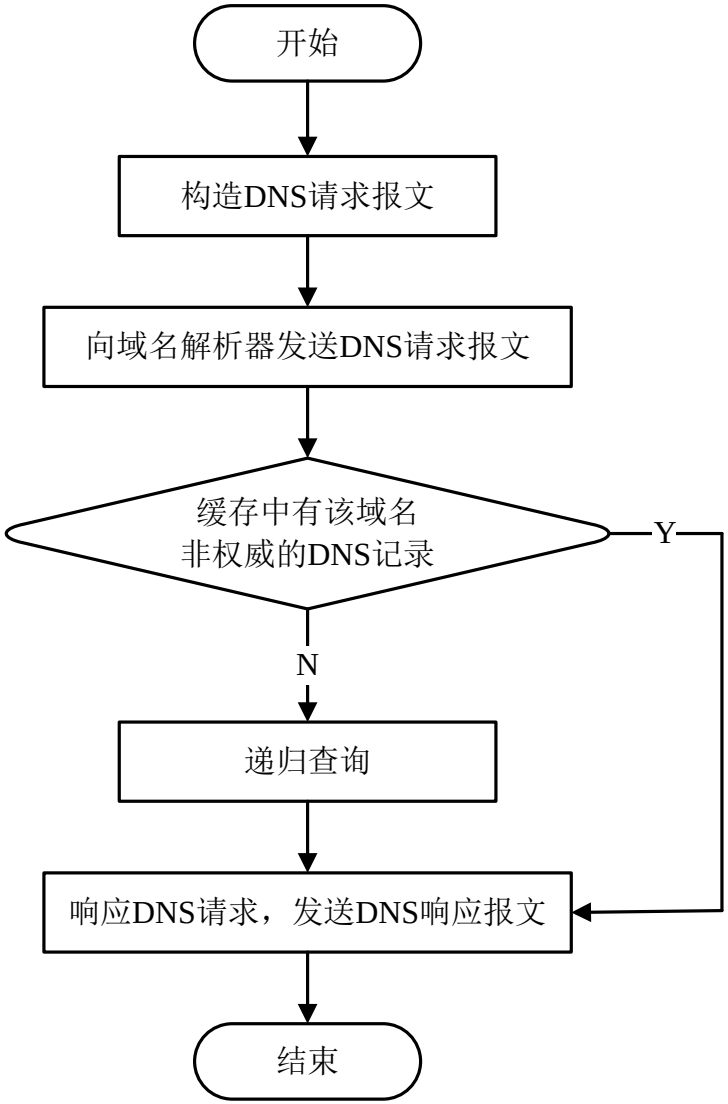
域名系统

域名解析流程

✦当解析一个域名时，用户需要首先构造DNS请求报文，并访问域名解析器。如果域名解析器缓存中有此域名非权威的DNS记录，则立即响应用户的DNS查询请求，将此域名非权威的DNS记录返回给用户。否则，域名解析器需要通过**递归查询**，依次访问各级域名服务器，以获得此域名权威的DNS记录，再将DNS响应报文发送给用户。

域名系统

域名解析流程


开始
构造DNS请求报文
向域名解析器发送DNS请求报文
缓存中有该域名
非权威的DNS记录
Y
N
递归查询
响应DNS请求，发送DNS响应报文
结束

域名系统

域名解析流程

以域名www.example.com为例，域名解析器进行递归查询的具体步骤如下：

✦用户请求域名解析器，解析域名www.example.com；

✦域名解析器缓存中没有该域名非权威的DNS记录，开始进行递归查询，访问根域名服务器，请求解析该域名；

✦根域名服务器上维持有一级域名.com的NS类DNS记录，将该NS类DNS记录，即一级域名.com的域名服务器IP地址返回给域名解析器；

✦域名解析器访问.com一级域名服务器，请求解析该域名；

域名系统

域名解析流程

✦.com一级域名服务器上维持有二级域名.example.com的NS类DNS记录，将该NS类DNS记录，即二级域名.example.com的域名服务器IP地址返回给域名解析器；

✦域名解析器访问.example.com二级域名服务器，请求解析该域名；

✦.example.com二级域名服务器上维持有域名www.example.com的A类DNS记录，将该A类DNS记录，即域名www.example.com对应的主机的IP地址返回给域名解析器；

✦域名解析器响应用户请求，将域名www.example.com对应的主机的IP地址返回给用户，完成递归查询。

域名系统

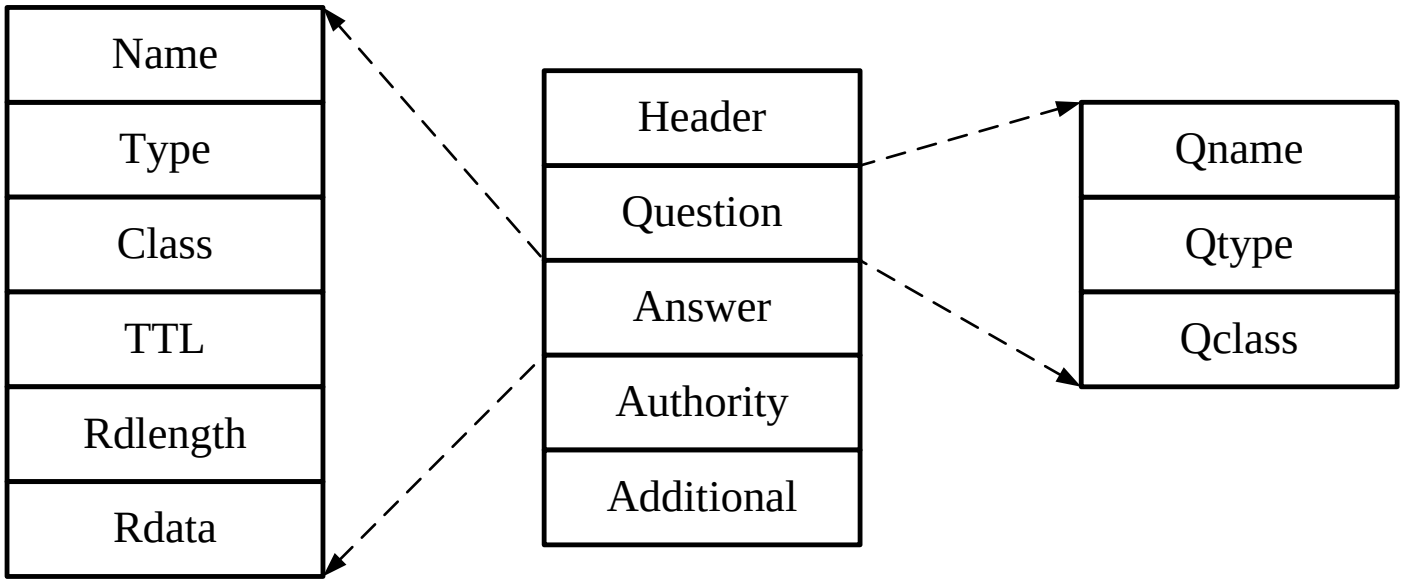
☙域名解析流程

✦从上面的例子可以发现，在递归查询过程中，域名解析器到各级域名服务器的RTT（Round Trip Time）和用户到域名解析器的RTT决定了解析一个域名所需要的时间。

域名系统

DNS协议

✦RFC 1035中详细阐述了DNS协议。DNS协议主要使用UDP协议通过53号端口收发DNS数据包。**DNS数据包结构**由Header、Question、Answer、Authority和Additional五个字段组成。**Header字段决定了DNS数据包的类型以及其它信息。**



域名系统

DNS协议

- DNS数据包分为**DNS请求报文**和**DNS响应报文**两类。
- DNS请求报文仅由一个UDP数据包组成，主要使用Header字段和Question字段。Question字段指示了DNS请求报文所请求解析的信息，包括请求解析的域名（Qname）、请求解析的DNS记录的类型（Qtype，例如0x0001代表A类DNS记录）和查询类型（Qclass，例如0x0001代表互联网地址）。

域名系统

DNS协议

✦在通常情况下，DNS响应报文也是一个UDP数据包，主要使用Header字段、Question字段和Answer字段；只有当DNS响应报文的大小超过512字节或域名服务器之间进行“Zone Transfers”的情况下，DNS协议才使用TCP协议进行数据传输。

✦在DNS响应报文中，Answer字段指示了DNS响应报文所返回的查询结果，包括所解析的域名（Name）、所返回DNS记录的类型（Type，例如0x0001代表A类DNS记录）、查询类型（Class，例如0x0001代表互联网地址）、所返回DNS记录的TTL值（TTL）、所返回查询结果的大小（Rdlength，即Rdata的大小）和所返回的查询结果（Rdata）。

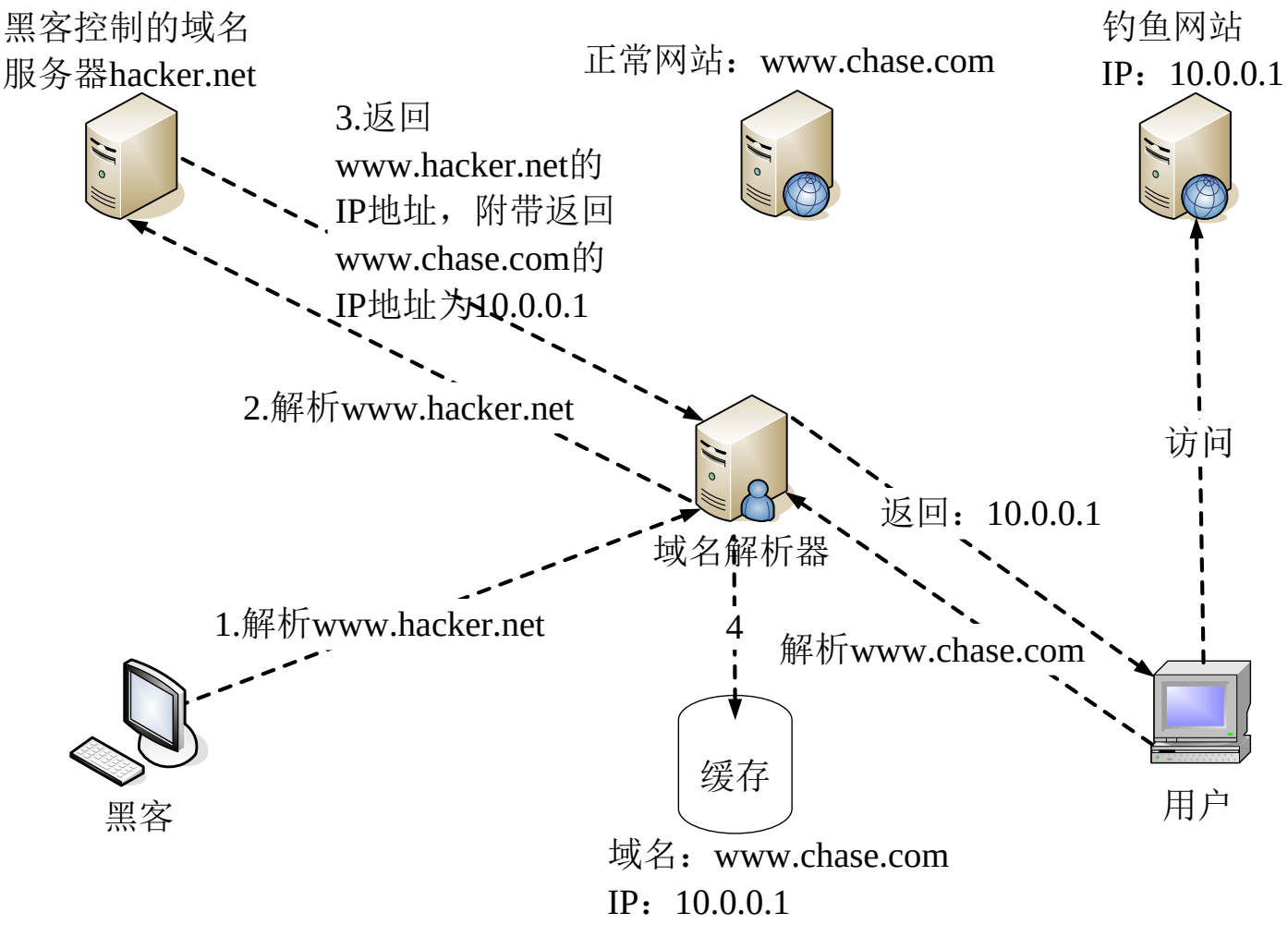
域名系统

DNS存在的一些问题

- 未缓存DNS记录的查询延迟
- TTL机制造成的更新延迟
- DoS攻击及网络故障的应变能力
- 管理复杂性及配置错误
- 域名解析器端故障
- DNS滥用

域名系统

DNS存在的一些问题



域名系统

新兴的域名服务系统

- ✦基于IP Anycast的域名服务器（如，UltraDNS， DynDNS）
- ✦基于IP Anycast的域名解析器（如，Google Public DNS，OpenDNS）