UDP协议应用实例之域名系统

因特网域名系统

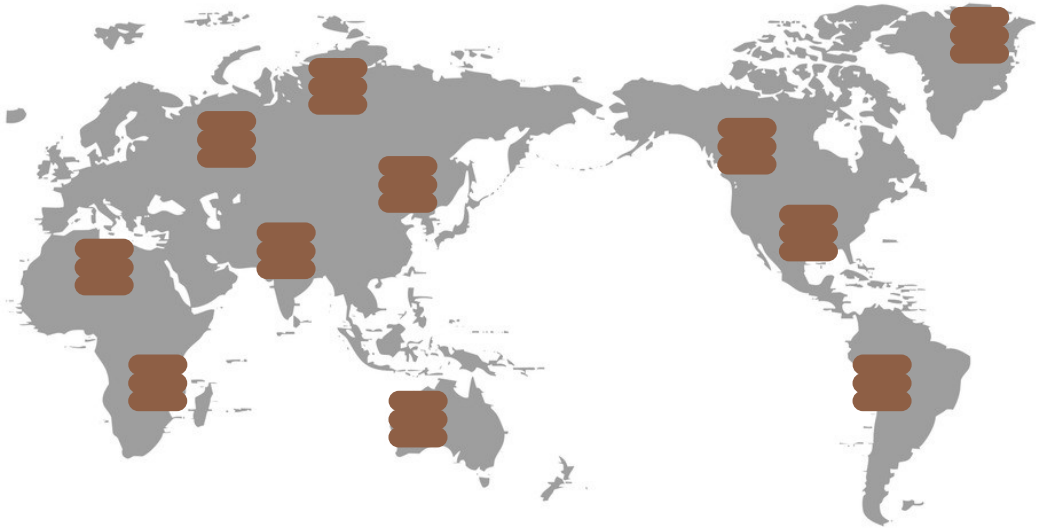
域名：用来表示主机、电子邮箱、服务器等便于记忆的名字，该名字特定于某个域，具有因特网全局唯一性。

RFC 1034
RFC 1035

DNS特点

- 层次的
- 分布式的
- 基于自治域

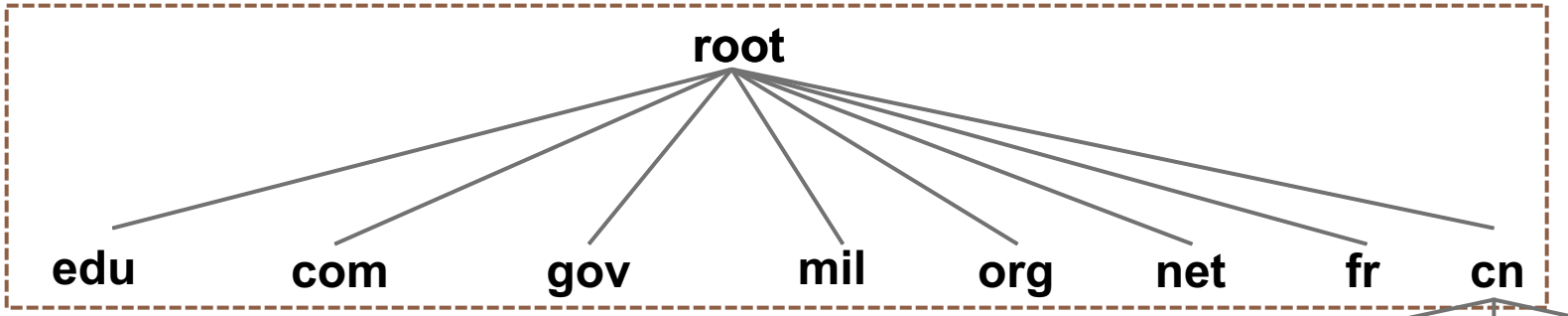
域名系统（DNS）：将主机名、电子邮件地址、Web服务器名等映射成IP地址的分布式数据库系统。



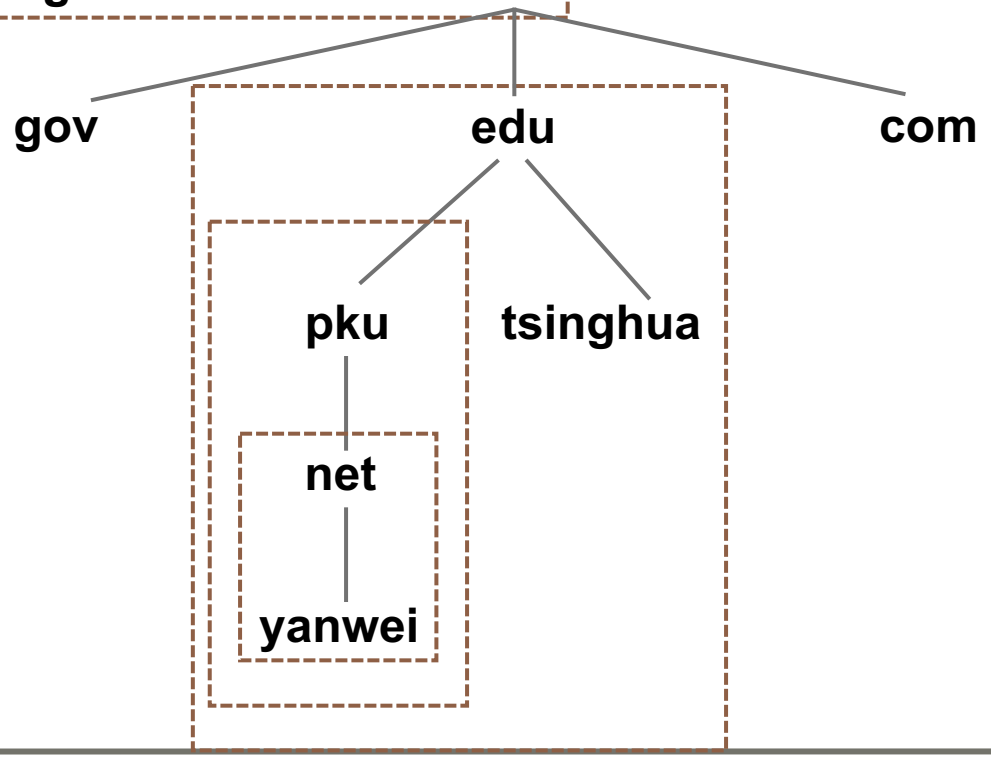
DNS是一个庞大的分布式数据库系统

名字的层次空间

● 顶级域名
(中国)



● 二级域名
(中国教育科研网)



中国北京大学网络实验室严伟
yanwei.net.pku.edu.cn

● 三级域名
(北京大学)

● 四级域名
(网络所)

?

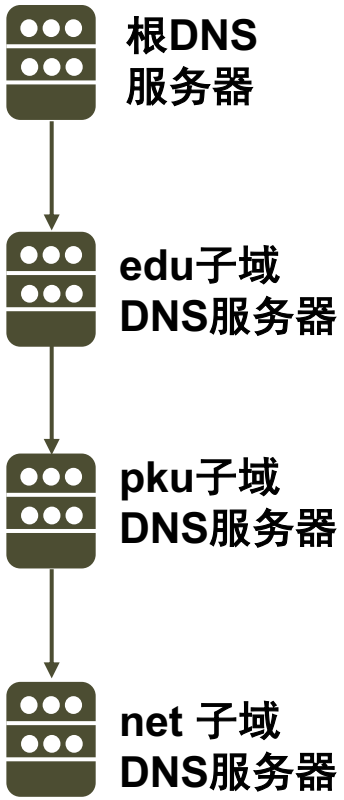
①如何存储全世界域名
②采取何种查询策略

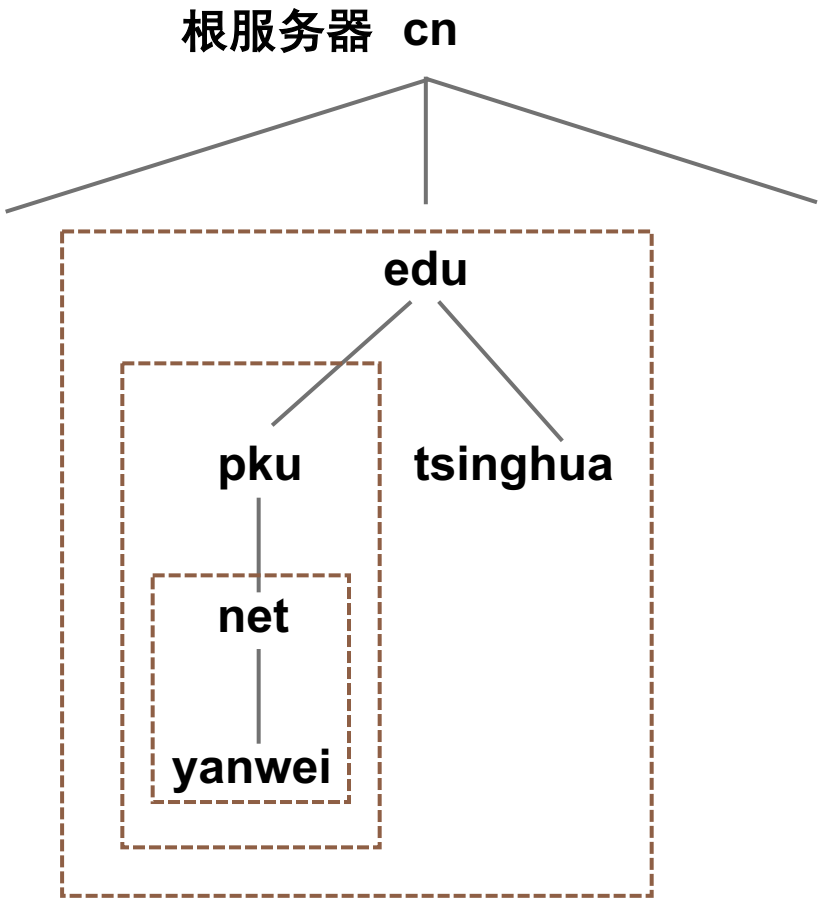
名字层次空间的管理

根服务器：它的管理区域是组成整棵树的服务器，这些服务器是得到授权的服务器。

授权服务器

- 域是一个“行政管理空间”
- 每个域有个负责该域空间名字的授权中心
- 域管理员负责域名空间的命名
- 域名解析授权可由父传给子节点





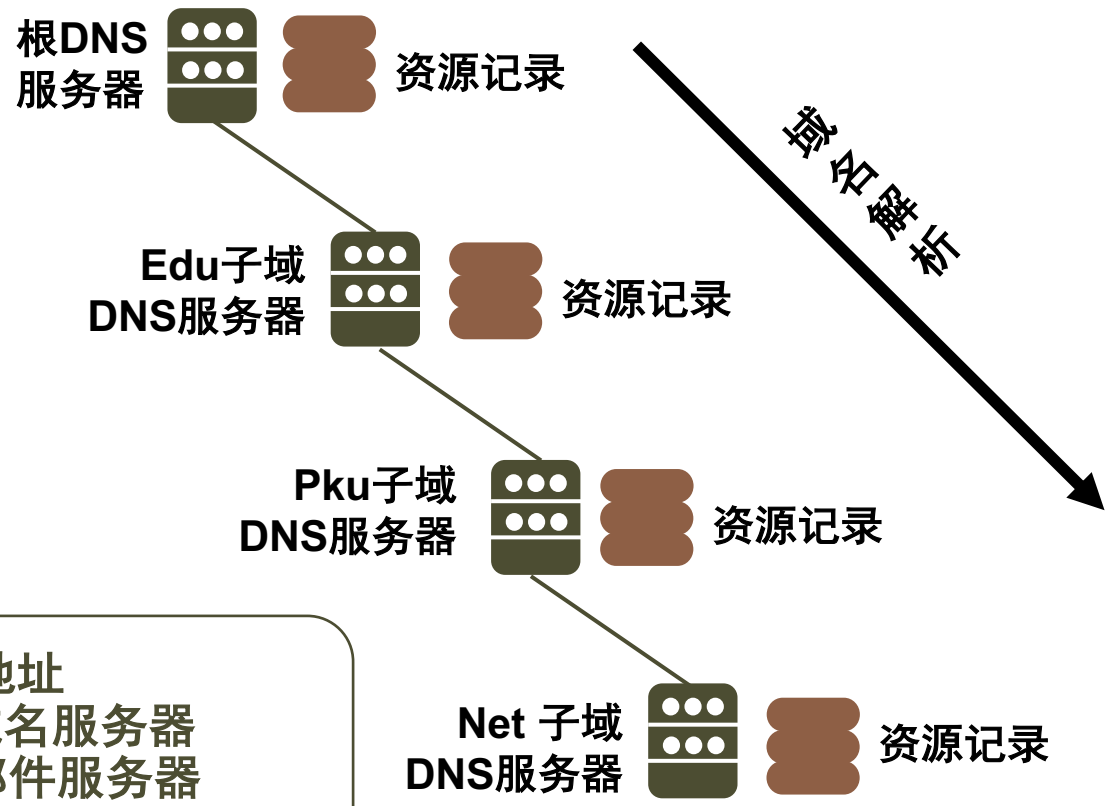
域名解析服务

域名解析：给定一个域名解析出其对应的IP地址的过程。

资源记录：给出了名字和IP地址的绑定或映射关系，是一个5元组。

- 名字 (name)
- 值 (value)
- 类型 (type)
- 分类 (class)
- 生存期 (TTL)

A：IP地址
NS：域名服务器
MX：邮件服务器
CNAME：主机规范名



DNS服务器维护一张资源记录表，响应针对本域名字的解析请求。

DNS主要功能

- 提供名字和地址的映射关系
- 指向子域的DNS服务器
- 提供各类主机别名
  - 例如：邮件服务器别名
  - 别名一般比规范名更易于记忆
  - DNS可返回对应的规范名和IP地址
- 提供负载均衡
  - 例如：www.sina.com.cn 对应多个具有不同IP地址的服务器
  - DNS数据库包括所有的IP地址
  - 每次DNS查询将获得该组IP地址但次序是循环的

Non-authoritative非授权：高速缓存内的信息，曾经收到过的查询结果。

DNS的资源记录与高速缓存

高速缓存

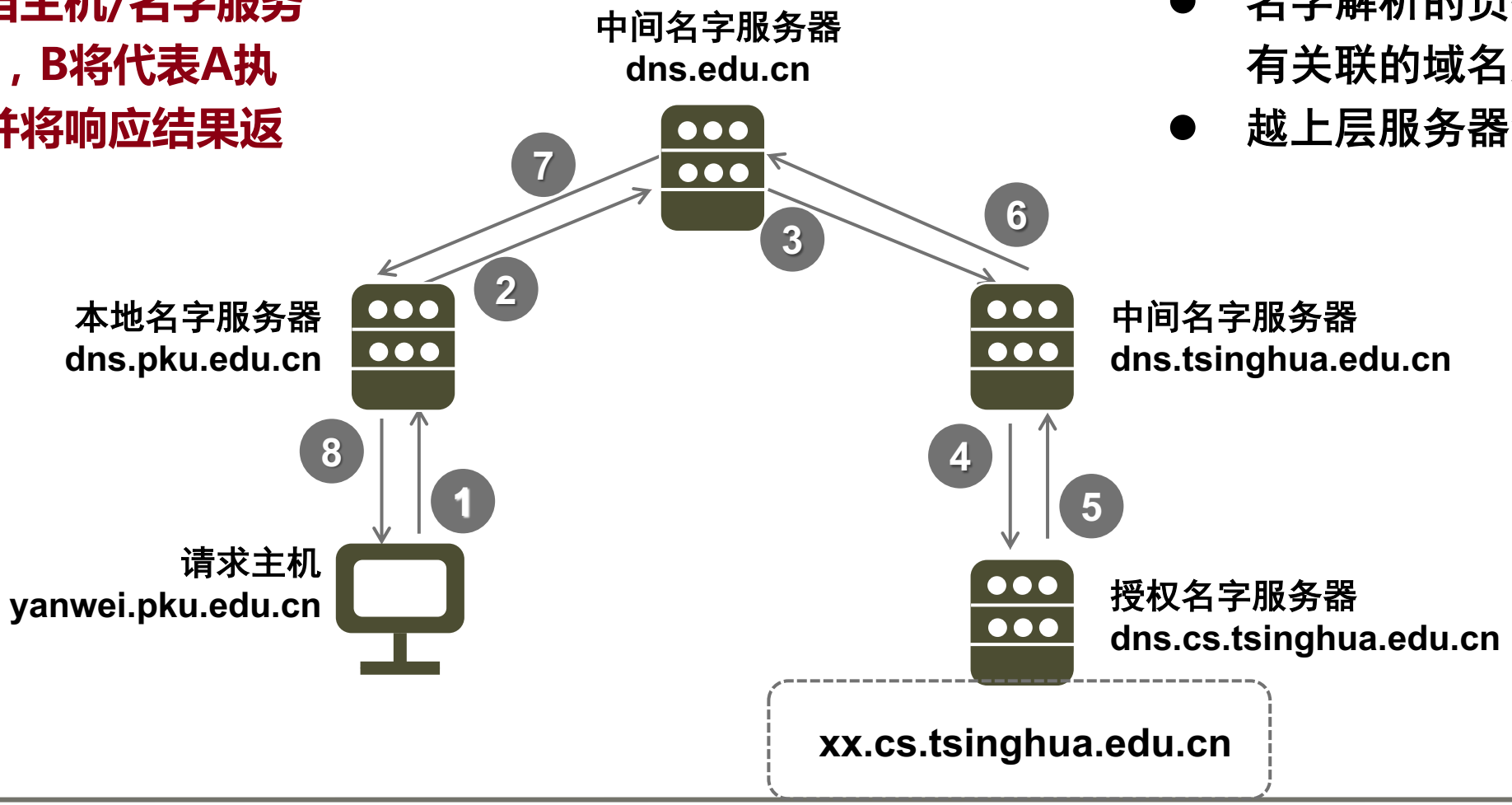
- DNS服务器在向请求方返回查询结果时，将查询结果存储在高速缓存中。
- 后续客户发出同样请求，则直接返回缓存结果，但同时声明这个查询结果来自高速缓存，即解析结果是非授权的。

Name	Value	Type	TTL
主机名	对应的IP地址	A	生存期
(net.pku.edu.cn, 162.105.203.25, A, two days)			
域名	域内授权名字服务器	NS	同上
(net.pku.edu.cn, dns.net.pku.edu.cn, NS, two days)			
主机别名	对应的规范名	CNAME	同上
(www.net.pku.edu.cn, net.pku.edu.cn, CNAME, two days)			
邮件别名	对应的规范名	MX	同上
(mail.net.pku.edu.cn, net.pku.edu.cn, MX, two days)			

*注意：表格中省却了分类 (IN)字段

DNS查询——递归查询

递归查询：当主机/名字服务器A向B查询，B将代表A执行查询请求并将响应结果返回给A。

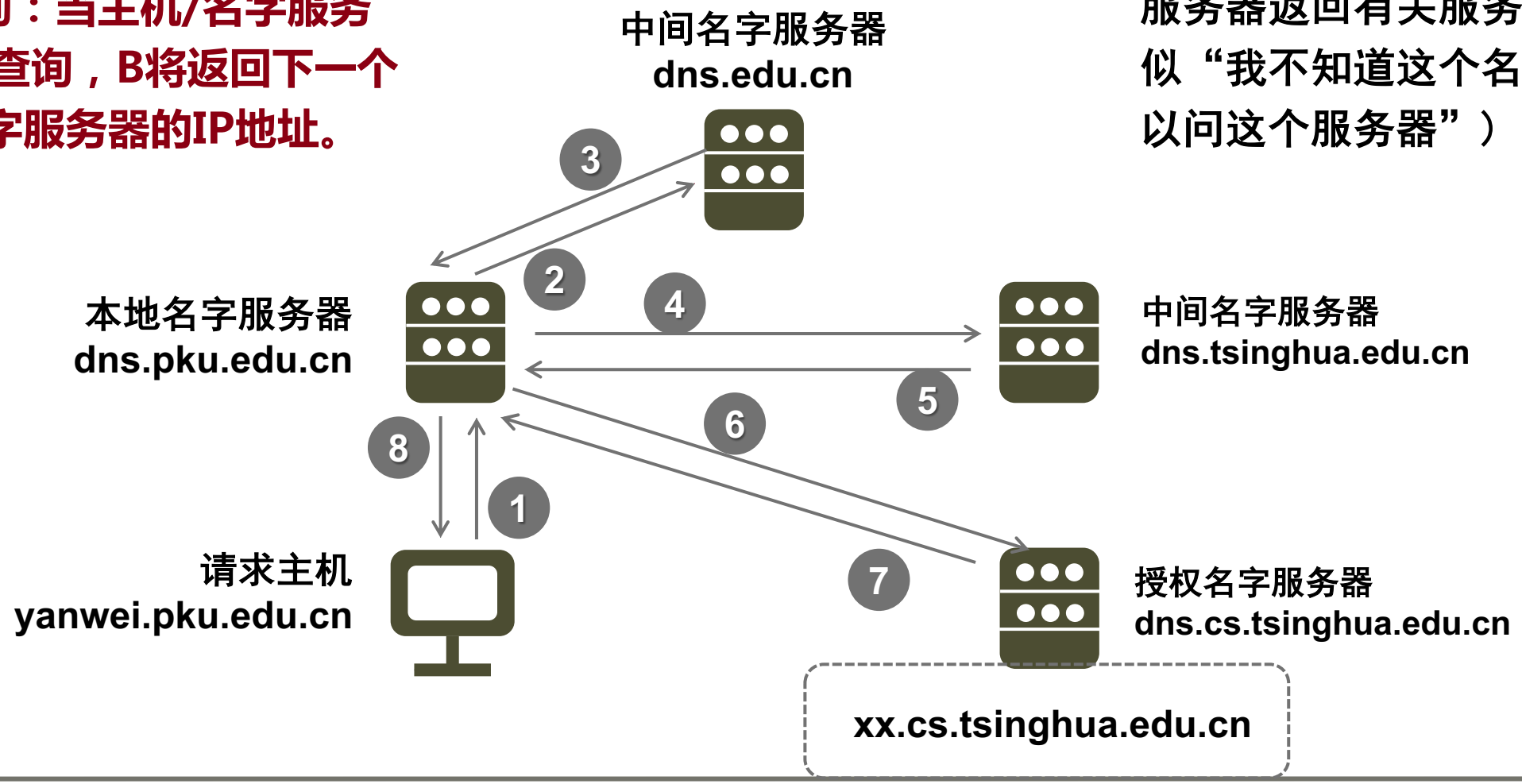


- 名字解析的负担加到所有关联的域名服务器
- 越上层服务器负担越重

DNS查询——迭代查询

迭代查询：当主机/名字服务器A向B查询，B将返回下一个DNS名字服务器的IP地址。

服务器返回有关服务器名字（类似“我不知道这个名字，你可以问这个服务器”）



DNS报文格式——报文头

16b	16b
Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
有效载荷（查询/响应）	

- Identification：标识本次查询，将被copy至reply报文；
- Flags：标识报文类型、响应类型和解析类型
- Questions#：请求报文中的查询域名数
- Answer RR#：响应报文中的资源记录数
- Authority RR#：授权记录数
- Additional RR#：额外记录数

报文类型
- query(0)
- reply(1)

响应类型
- Authoritative: 返回的结果来自授权服务器

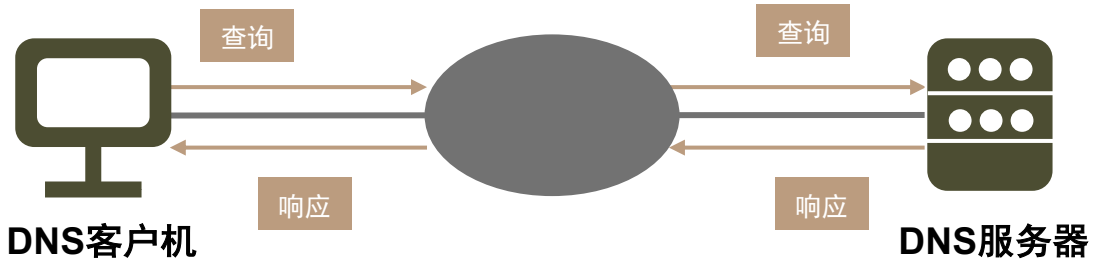
解析类型
- Recursion: 递归查询
- iterative：迭代查询

DNS报文格式——报文正文

Questions (variable number of questions)
Answers (variable number of resource records)
Authority (variable number of resource records)
Additional Information (variable number of resource records)

- 查询字段由一条或多条查询记录数组成，查询记录包括DNS客户机请求解析的域名
- 响应字段由一条或多条资源记录组成，用于DNS服务器对查询请求的应答
- 授权字段由一条或多条资源记录组成，用于查询某个域的一台或多台服务器的域名
- 额外信息由一条或多条资源记录组成，用于解析指定域的授权DNS服务器域名及其IP地址

DNS报文的传递



- 当响应报文长度小于512字节时用UDP协议
- 当响应报文长度大于512字节时用TCP协议
- 无论用哪种协议，DNS服务器端口号均为53

DNS报文头

Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
有效载荷（查询/响应）	

可变长的DNS查询/响应报文正文

Questions (variable number of questions)
Answers (variable number of resource records)
Authority (variable number of resource records)
Additional Information (variable number of resource records)