第七章 应用层

# DNS 解析

# 为什么需要域名解析？

封装的过程

信息、数据流、数控段、数据分组、数据帧、比特流

只知道被访问资源的域名，而不知道对用的IP地址时

由域名服务器提供解析服务

# 什么是域名解析？

- 将域名映射为IP地址的方法和过程
- DNS的使用方法：
  - 为了将一个名字映射为IP地址，应用程序调用一个叫解析器（ resolver ）的库过程，把名字作为参数传递给这个过程（如：gethostbyname()就是一个解析器）
  - 解析器发送一个UDP分组给本地DNS服务器，它会负责查找该名字，然后将对应的IP地址返回给解析器
  - 解析器返回结果给应用程序，然后应用程序即可开始工作了（封装，发送……）

# 域名解析

- 当一个解析器收到一个域名查询时，它将该查询传递给本地的一个域名服务器
- 如果待查询的域名落在该名字服务器的管辖范围内，它将返回权威资源记录
  - 一个权威资源记录（authoritative record）是指来自于管理该记录的权威机构，因此总是正确的，它和缓存的记录不同，后者可能是过期的
- 如果被请求的域名是远程的，且本地没有关于它的信息，那么本地名字服务器向根域服务器发送一条查询此域的消息

# 域名解析的种类

## 主机向本地域名服务器

查询一般都是采用递归查询。

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

本地域名服务器以 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

# 域名解析的种类

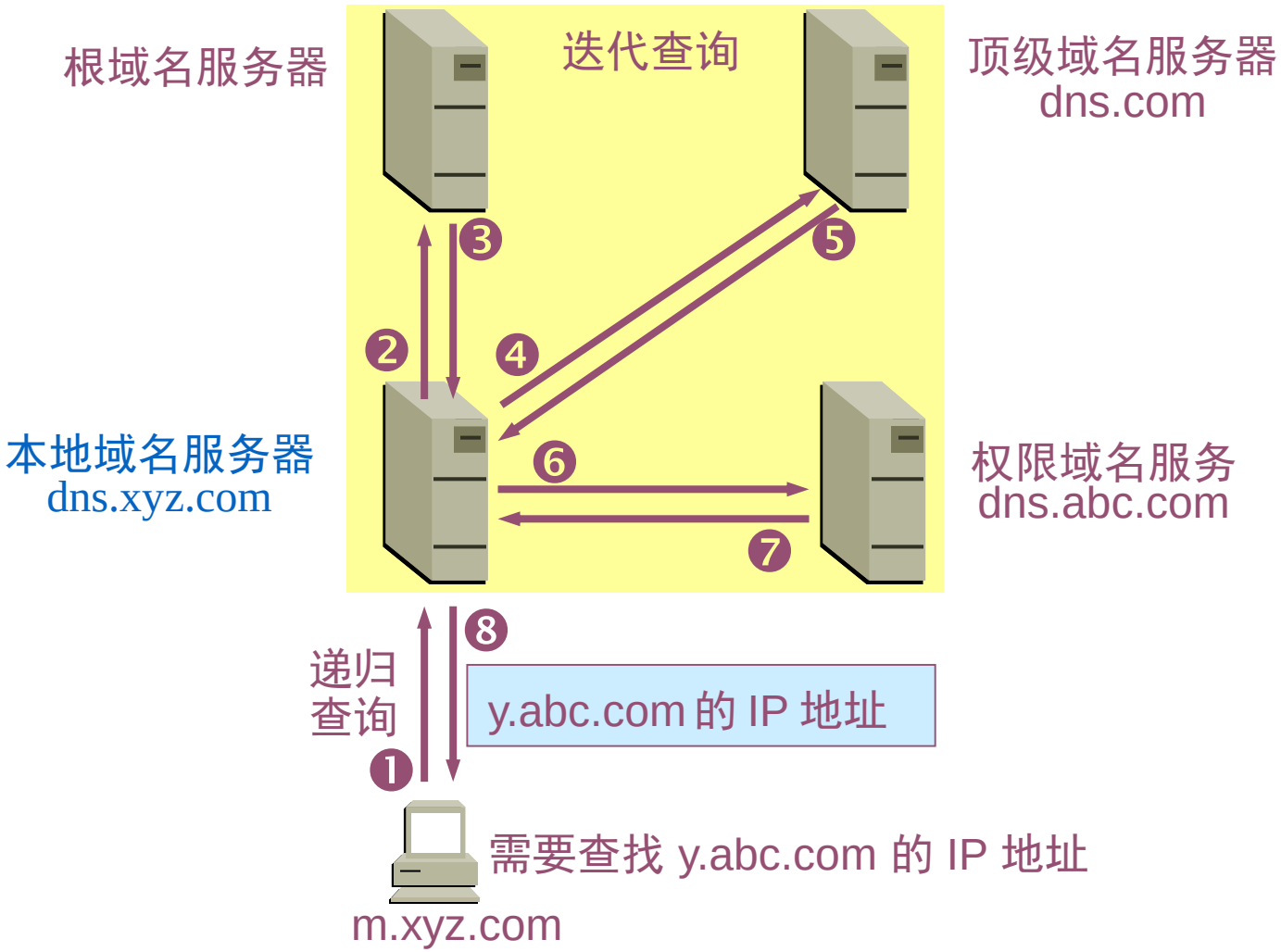
**本地域名服务器向根域名服务器**

查询通常是采用迭代查询。

根域名服务器收到本地域名服务器的迭代查询请求报文

- 给出所要查询的 IP 地址
- 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” → 本地域名服务器进行后续的查询

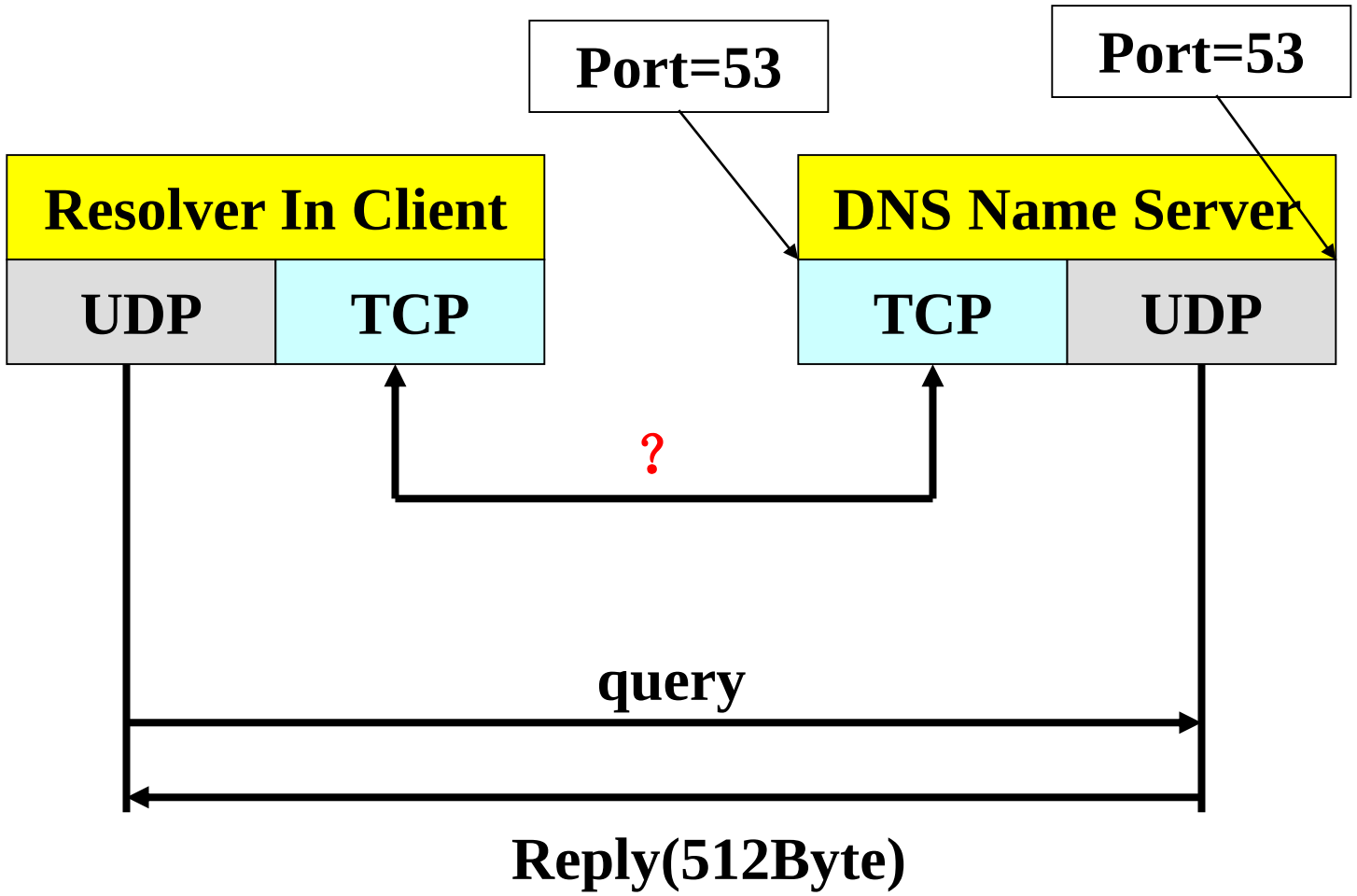
# 一次完整的解析


根域名服务器
迭代查询
顶级域名服务器
dns.com
本地域名服务器
dns.xyz.com
权限域名服务
dns.abc.com
递归
查询
y.abc.com 的 IP 地址
需要查找 y.abc.com 的 IP 地址
m.xyz.com

# 优化方法

- 高速缓存—减少查询环节，提高效率
  - 上例中，本域中的另一台主机如果查询同一个域名，则马上可得到结果
  - 上例中，本域中的另一台主机如果查询另一个域名，如Z.abc.com，则可直接发送到权威域名服务器得到权威记录
- 缺点：缓存中的内容不具有权威性

# DNS消息传递


Port=53
Port=53
Resolver In Client
DNS Name Server
UDP
TCP
TCP
UDP
?
query
Reply(512Byte)

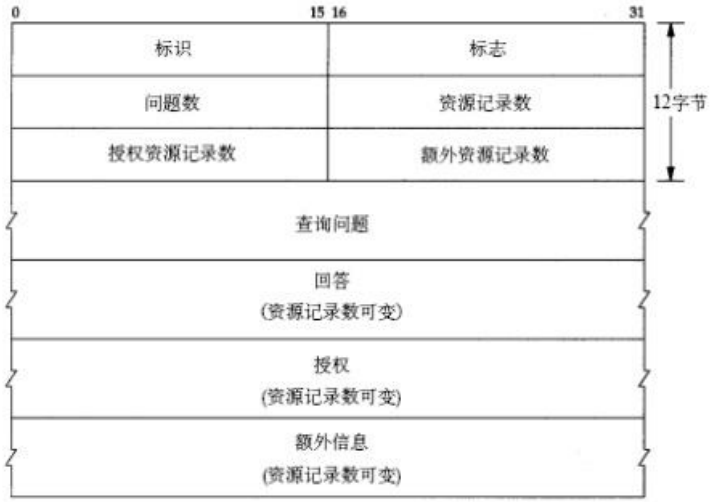
# 什么时候使用TCP?

## UDP报文超过512Bytes

- 对首次请求响应，返回参数TC置位
- 再请求，建立TCP连接，将数据流分段发送

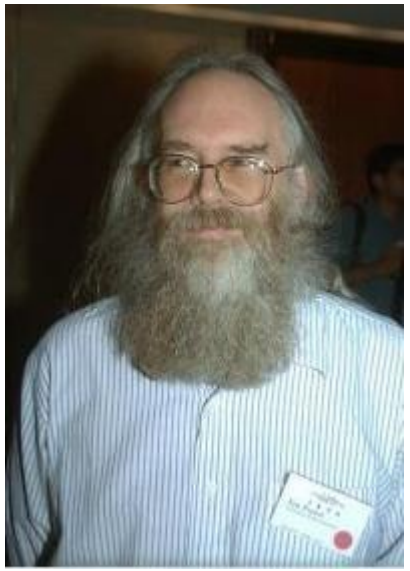
## 从(second)服务器的数据更新

- 主、从 服务器间建立TCP连接
- 进行批量数据流传输



# DNS是否存在不安全的因素？

ICANN诞生前，TLD主要由IANA的Prof.Jon Postel负责



- M 根域在日本
- IQ的授权与被删除事件
- Internet  society 信任Postel
- Jon Postel 于1998年劫持了根域服务器

# 小结

- 域名解析是将域名映射为IP地址的方法和过程
- 一次完整的域名解析包括递归解析和迭代解析
- 通过各级缓存优化查询，所获得的解析结果可能无效
- DNS存在不安全的因素

# 思考题

- 为什么需要域名解析？
- 什么是域名解析？
- 一次完整的域名解析是怎样的？
- 当本地域名服务器无法给出解析结果时，怎么办？
- 怎样优化域名解析，提高解析效率？
- DNS可能出现什么安全问题？试查询曾经出现过的DNS安全事件。

# 谢谢观看

# 致谢

本课程课件中的部分素材来自于：（1）清华大学出版社出版的翻译教材《计算机网络》（原著作者：Andrew S. Tanenbaum，David J. Wetherall）；（2）思科网络技术学院教程；（3）网络上搜到的其他资料。在此，对清华大学出版社、思科网络技术学院、人民邮电出版社、以及其它提供本课程引用资料的个人表示衷心的感谢！

对于本课程引用的素材，仅用于课程学习，如有任何问题，请与我们联系！