2023InForSec夏令营

互联网域名系统安全

An Overview of Domain Name System Security

陆超逸

清华大学 网络科学与网络空间研究院 博士后

2022年8月1日 @ 中国海洋大学

课程主要内容

一、域名系统的工作原理

二、域名系统的安全威胁

三、域名系统的安全防御

四、实践环节：缓存污染攻击

第一部分 Part I

域名系统的工作原理

网络上的数据包是怎样寻址的?

IP地址：互联网上计算机必备的身份标识

依据IP地址，通过路由协议到达目的主机

211.64.142.153

IPv4地址

2001:da8:7013:8104::8047

IPv6地址

IP地址的书写特点：由（十进制或十六进制）数字构成

优点：便于计算机处理

缺点：难以记忆或输入，对互联网用户不友好

思考：

你记得多少家人/朋友的电话号码?

我们目前怎么解决号码记不住的问题?

怎样让互联网对用户更加友好？

域名：互联网上计算机的身份标识，但是可读

互联网主机的**另外一套命名体系，便于记忆和输入**

（计算机：喵喵喵？？？无法直接处理）

思路：构建域名和IP地址之间的映射机制

用户输入域名，计算机处理IP地址

“通讯录式”映射机制：将所有映射关系统一硬编码

每台主机存储相同的映射关系文件，在本地完成域名到IP地址的转换

思考：

“通讯录式”映射机制有什么缺点？能在当前的全球互联网环境中使用吗？

域名到IP地址之间的映射机制一旦失效，会导致什么后果？

从认识域名开始

域名由若干个标签（label）组成，标签之间用点号（.）分隔

标签允许包含的字符：英文大小写字母、数字、短横线

标签4：www
代表www网页服务

标签3：ouc
代表中国海洋大学（Ocean University of China）

标签2：edu
代表教育行业

标签1：cn
代表中国

范围小 ← → **范围大**

从认识域名开始

域名由若干个标签（label）组成，标签之间用点号（.）分隔

标签允许包含的字符：英文大小写字母、数字、短横线

标签4：www
代表www网页服务

标签3：ouc
代表中国海洋大学（Ocean University of China）

标签2：edu
代代表教育行业

标签1：cn
代表中国

类比：倒过来的邮寄地址

三沙路.黄岛区.青岛市.山东省.中国

思考：

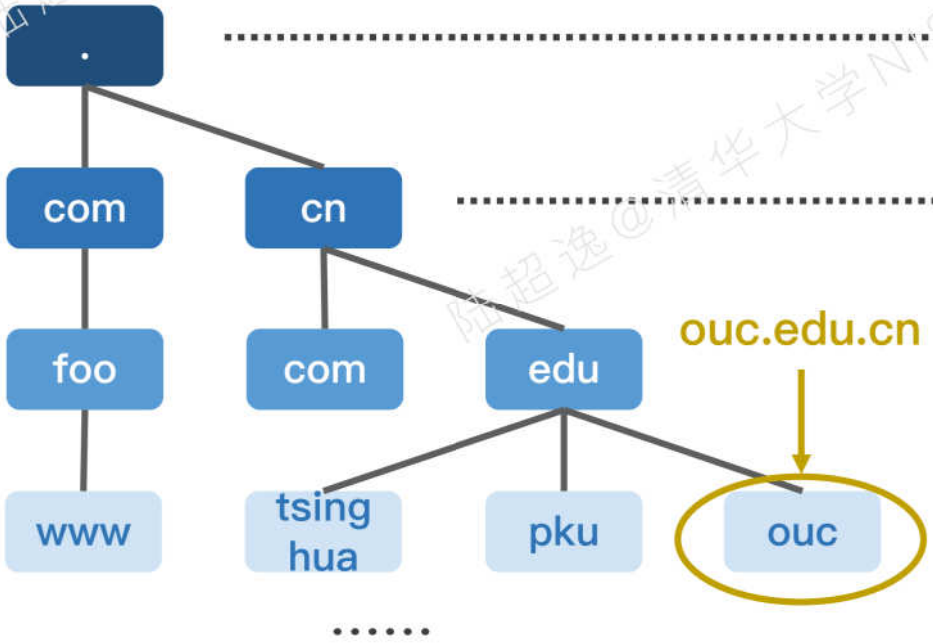
根据以上特征，可以用一个什么样的数据结构来管理互联网中的所有域名？

互联网域名空间

互联网域名空间呈现一个树形结构

唯一的根结点：根域名（用点号表示，在域名书写中通常省略）

确保域名具有排他性，是**互联网主机的命名空间**



根域名（root）
互联网域名空间的唯一起点

顶级域（TLD）
一般不开放给普通用户，目前有1480个左右

思考：
是否可以使用一个不存在的顶级域下的域名，比如wode.diannao?

1/6场休息，请回顾：

为什么互联网需要域名？

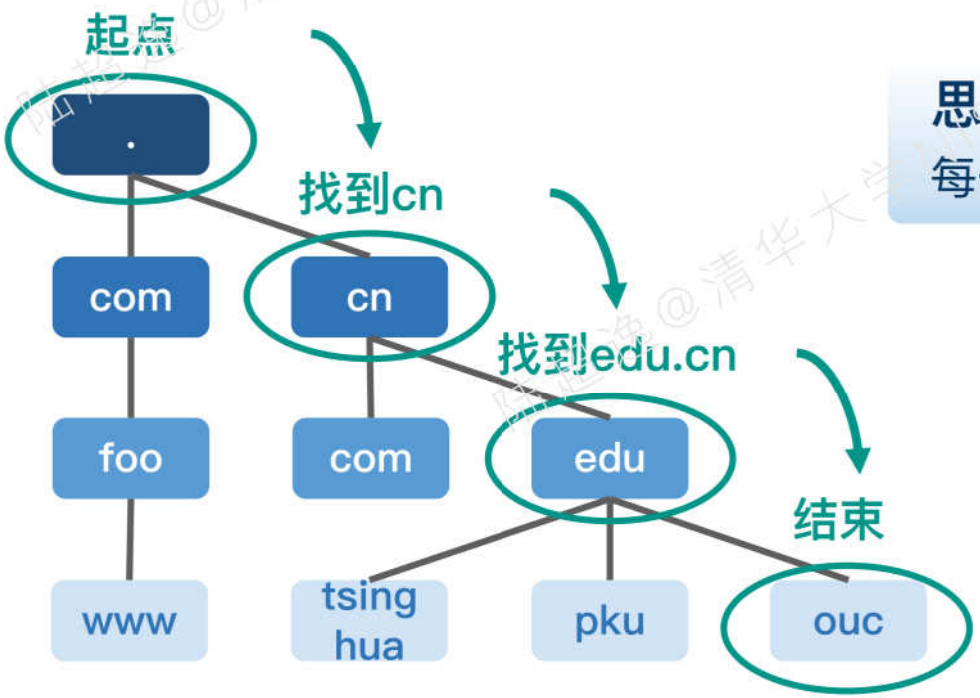
域名的构造规则是怎样的？

互联网域名空间是怎样的结构？

怎样查找一个域名?

怎样在域名空间中找到ouc.edu.cn?

以唯一的根域名为起点，**逐级向下**查找；在同一深度最多经过一个节点



思考：

每一步都能往下继续查找的条件是什么?

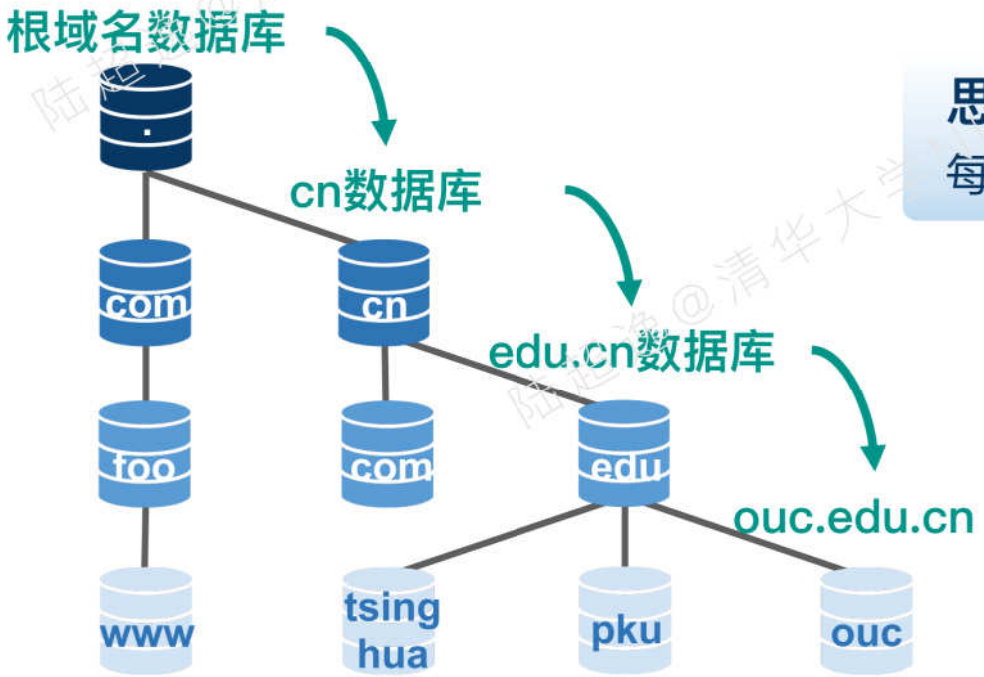
本级域名存在

能找到去往下一级域名的路径

怎样查找一个域名?

怎样在域名空间中找到ouc.edu.cn?

以唯一的根域名为起点，**逐级向下**查找；在同一深度最多经过一个节点



思考：

每一步都能往下继续查找的条件是什么?

每级域名各自维护数据库

数据库中存储自身的映射关系，以及所有下一级数据库的位置

域名数据库的内容：资源记录和区域

资源记录（RR）：域名映射关系的表示形式

域名	缓存时间	资源类别	资源类型	资源值
www.ouc.edu.cn	3600	IN（默认）	A	211.64.142.153

- www.ouc.edu.cn对应的IPv4地址是211.64.142.153
- 这条记录可以被域名服务器缓存1小时

常见的资源类型代号

资源类型	含义	资源类型	含义
A	IPv4地址	AAAA	IPv6地址
NS	权威服务器名称	MX	邮件服务器名称
CNAME	域名别名	SOA	起始授权信息

域名数据库的内容：资源记录和区域

区域（zone）：一系列资源记录构成的集合

某个域名的区域，一般指**和它相关的所有资源记录**（即它的完整“数据库”）

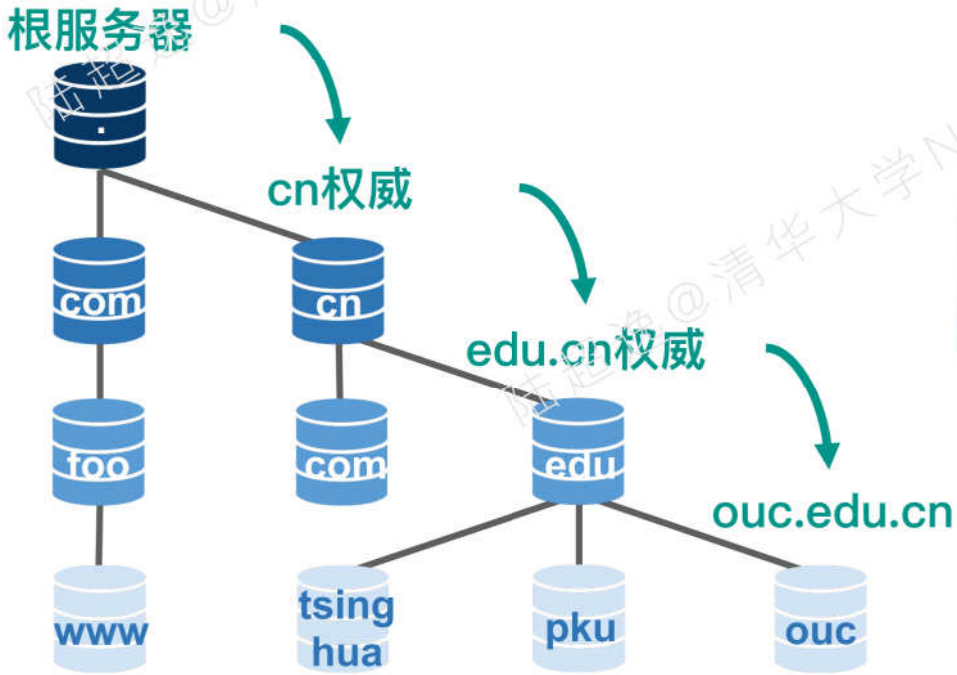
包含它的所有资源记录，也可能包含其子域名的资源记录（如“通往下一级的路径”）

域名edu.cn的区域（部分）				
edu.cn	**172800**	**IN**	**NS**	**dns.edu.cn**
• edu.cn自己的“数据库”由dns.edu.cn维护 • （edu.cn这个域名并没有指定IP地址，所以没有A/AAAA记录）				
ouc.edu.cn	**3600**	**IN**	**NS**	**dns.ouc.edu.cn**
• ouc.edu.cn（下一级）的“数据库”由dns.ouc.edu.cn维护				
dns.ouc.edu.cn	**3600**	**IN**	**A**	**211.64.142.16**
• ouc.edu.cn（下一级）的“数据库”所在的IP地址是211.64.142.16				

域名数据库的实现：权威服务器

权威服务器（Authoritative server）：维护“数据库”的实体机器

由域名所有者自行搭建（或外包），负责**存储区域、响应域名查询**



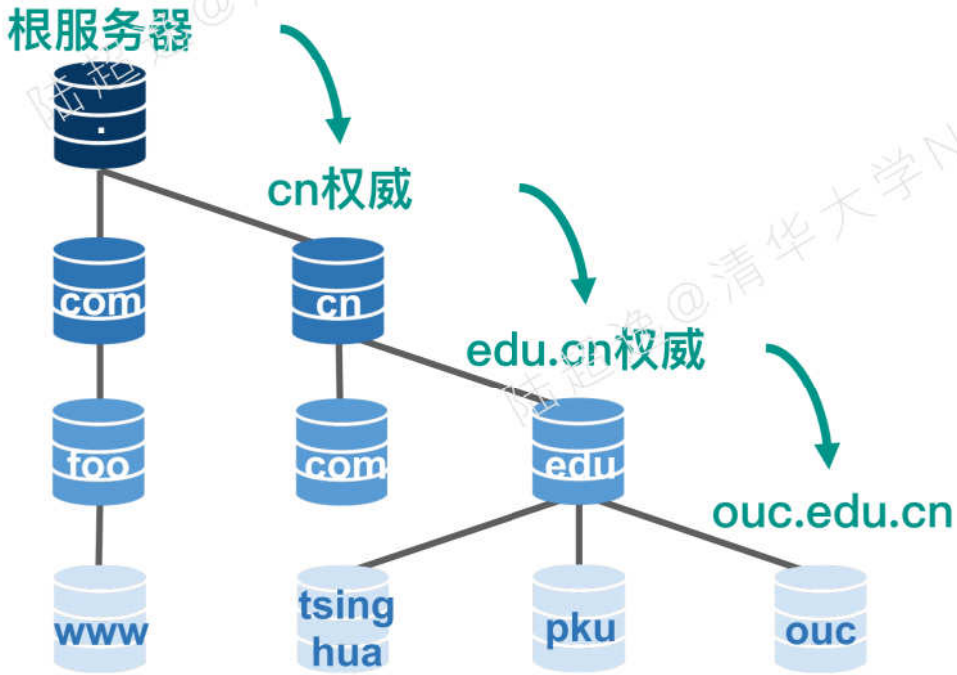
思考：

权威服务器的算法应该是什么样子的?

域名数据库的实现：权威服务器

权威服务器（Authoritative server）：维护“数据库”的实体机器

由域名所有者自行搭建（或外包），负责**存储区域、响应域名查询**



实验：

edu.cn的权威服务器是202.38.109.35

分别向它发送如下域名的解析请求：

- edu.cn（NS类型）
- ouc.edu.cn（A类型）
- ouc.org.cn（A类型）
- www.ouc.org.cn（A类型）
- cn（A类型）

观察结果，总结权威服务器的查找算法

根服务器：域名数据库查询的起点

全球共有13个根服务器地址，由12个独立机构管理

使用字母A–M表示

所有根服务器共享一份根区域文件，相互可替代

所有根服务器地址均部署任播（Anycast）技术

每个根服务器地址对应**多台完全一样的实体机器**（称为根服务器节点）

全球目前约有1500个根服务器节点

了解更多：https://root-servers.org

思考：

根服务器部署任播技术的好处有哪些？

一旦根服务器瘫痪，会有什么后果？

根服务器节点的全球分布

1/3场休息，请回顾：

为什么说互联网域名数据库是分布式的?

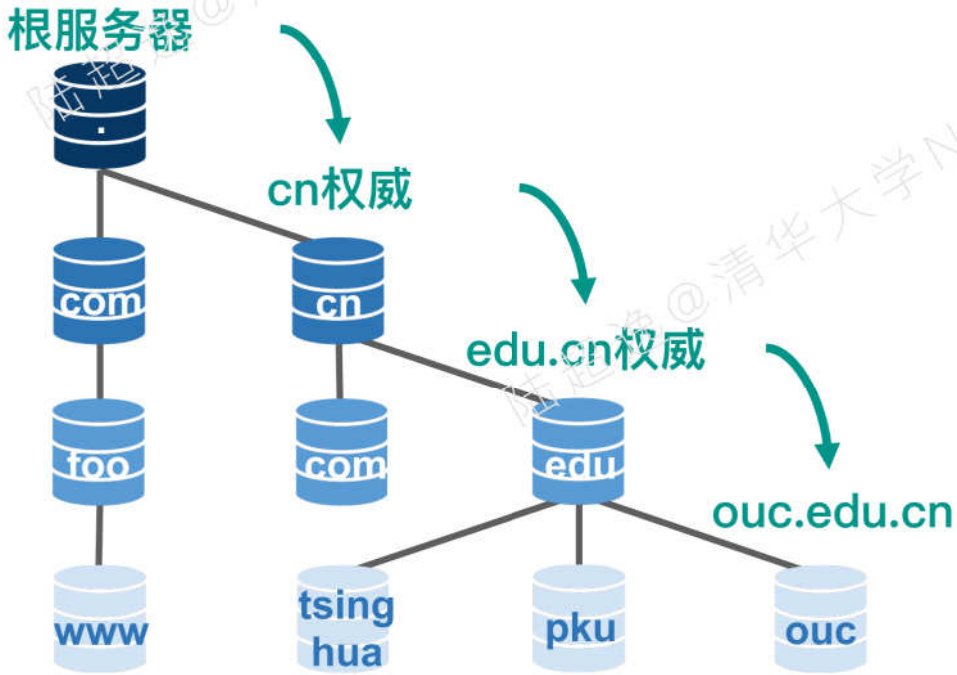
域名映射关系是怎样存储的?

根服务器是如何管理的?

互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**

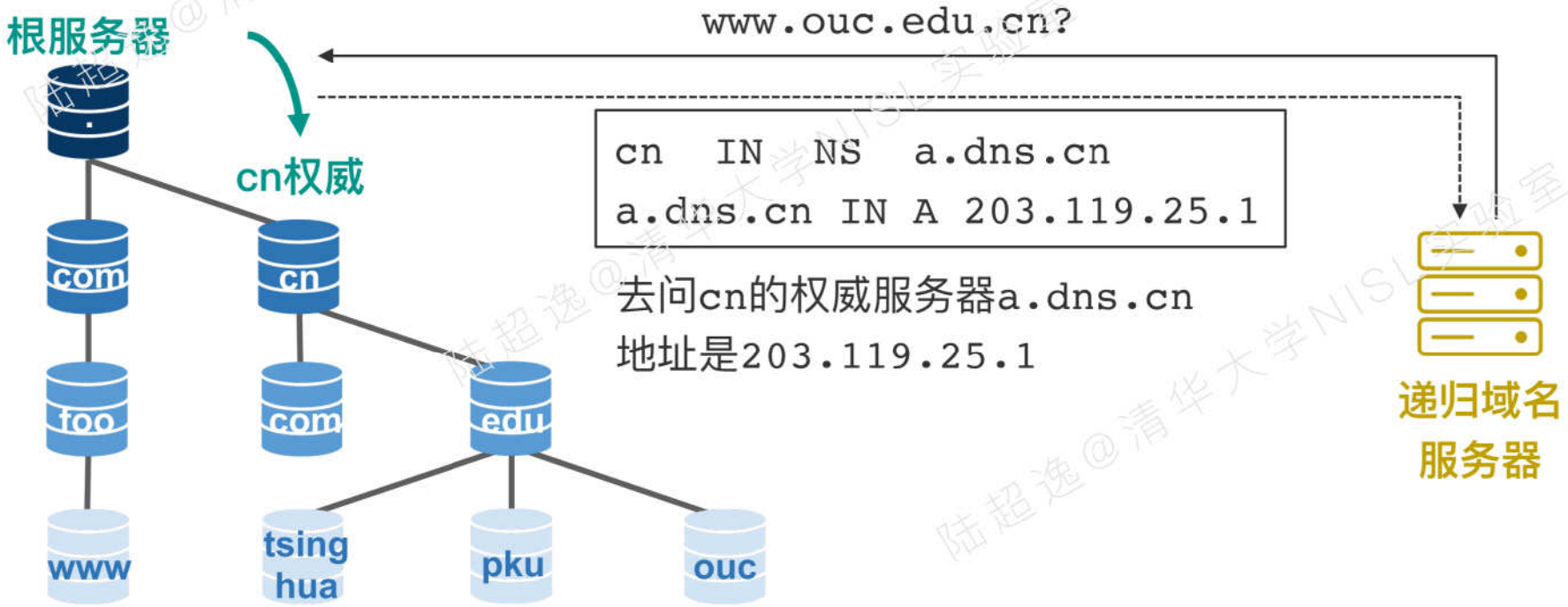


递归域名
服务器

互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

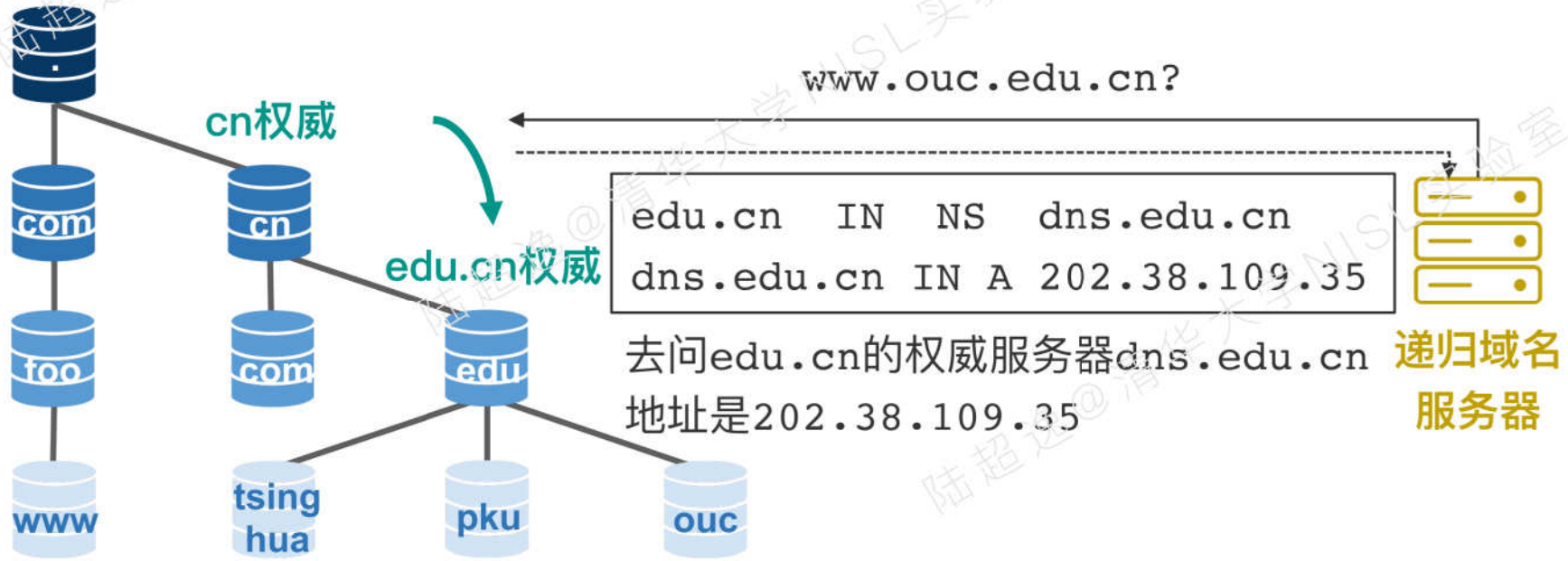
何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**



互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

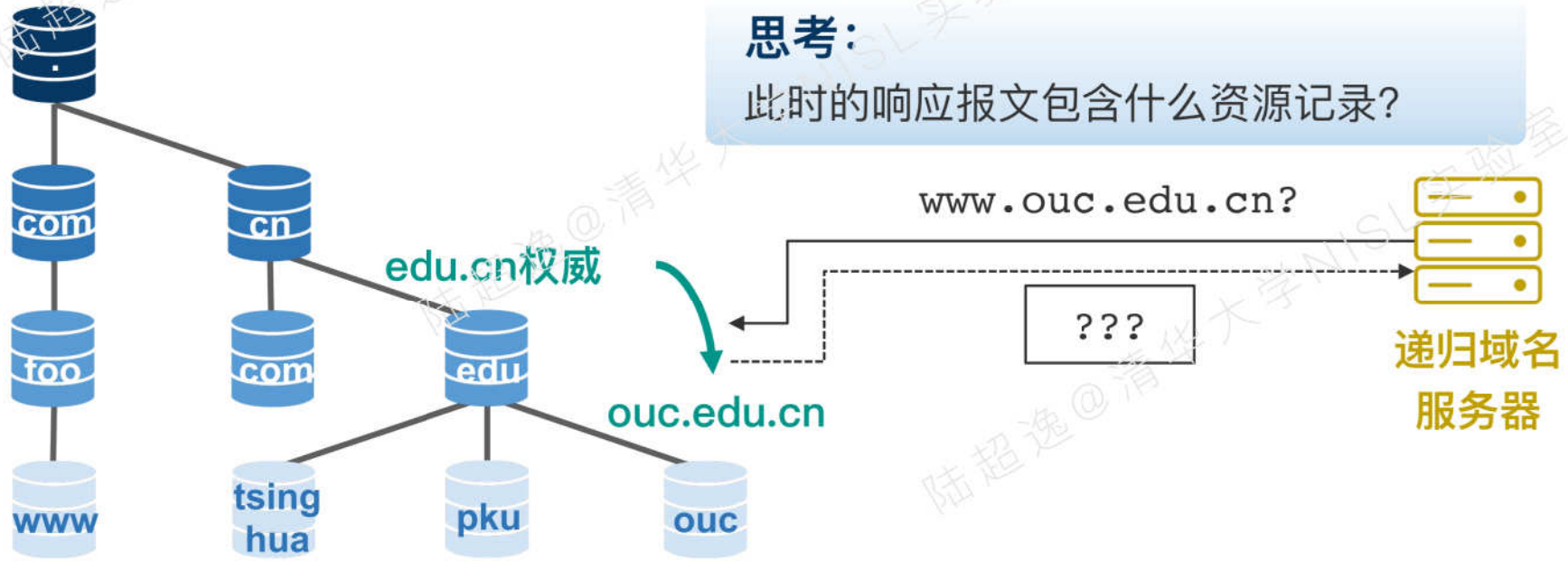
何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**



互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**



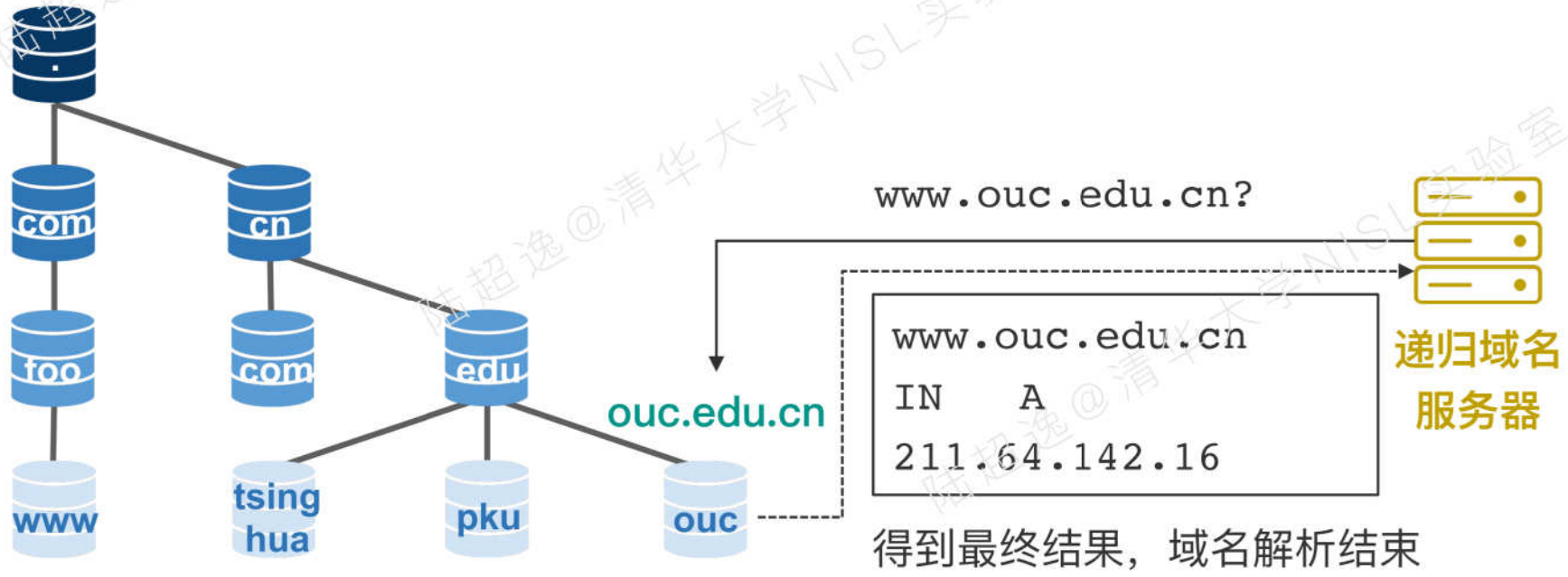
思考：

此时的响应报文包含什么资源记录？

互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**



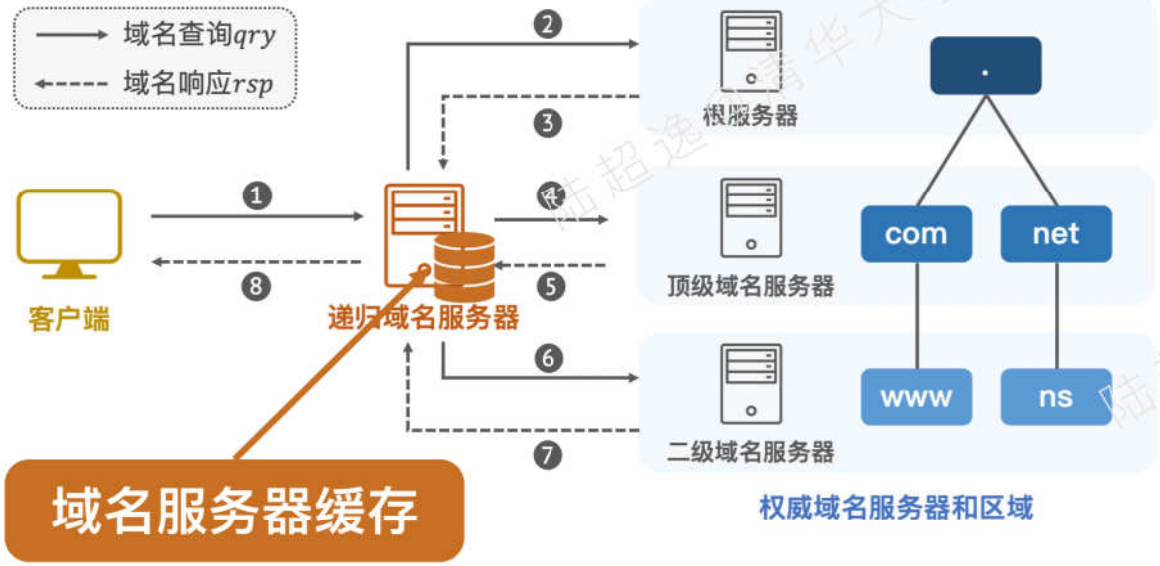
互联网域名的解析实现

递归域名服务器（recursive resolver）：全权代理域名解析操作

何谓“递归”：从根服务器开始，根据权威服务器提供的“线索”，**查到最终结果为止**

递归域名服务器默认情况下由接入网络随DHCP分配

也可由用户自行在操作系统中指定

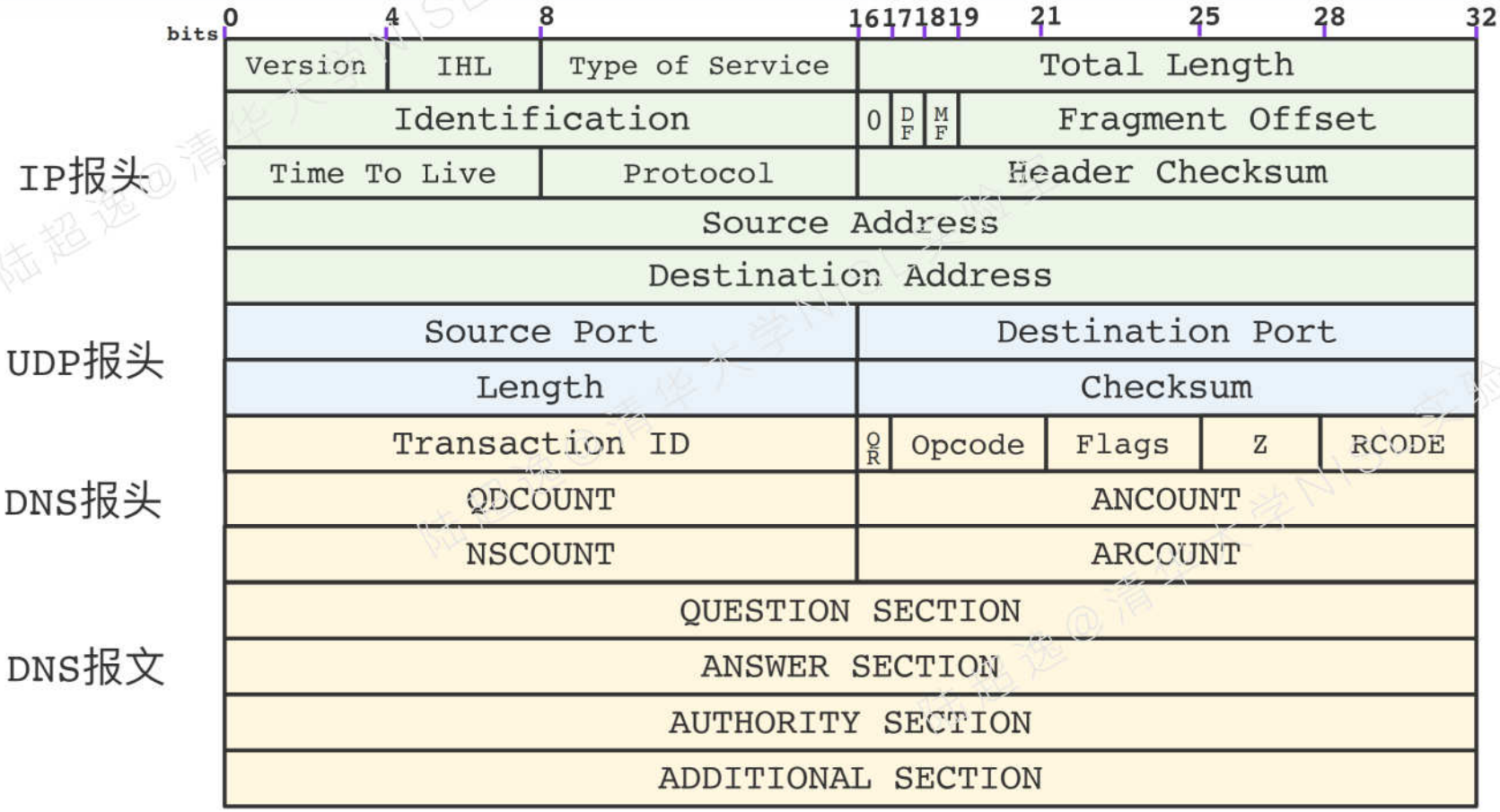


思考：

怎样找到根服务器？

怎样提高递归域名解析的性能？

域名解析报文格式


bits
0
4
8
16
17
18
19
21
25
28
32
IP报头
UDP报头
DNS报头
DNS报文
Version
IHL
Type of Service
Total Length
Identification
0
DF
MF
Fragment Offset
Time To Live
Protocol
Header Checksum
Source Address
Destination Address
Source Port
Destination Port
Length
Checksum
Transaction ID
QR
Opcode
Flags
Z
RCODE
QDCOUNT
ANCOUNT
NSCOUNT
ARCOUNT
QUESTION SECTION
ANSWER SECTION
AUTHORITY SECTION
ADDITIONAL SECTION

域名解析报文格式

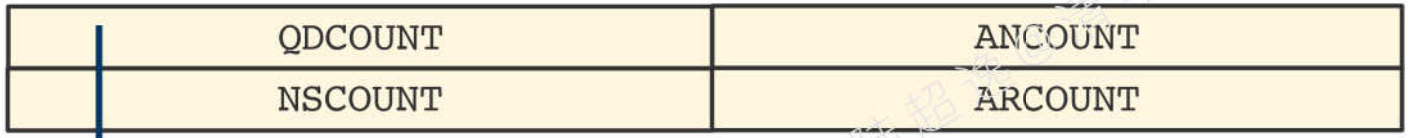
DNS报头字段及其含义

消息序号（TXID）
用于区分多个DNS报文

QR标记
这是请求还是响应报文

响应码
00查询成功
03域名不存在

标记
RD是否想进行递归查询；RA是否能进行递归查询
AA响应是否来自权威服务器；AD响应是否经过DNSSEC校验



区域条目计数
问题区域、回答区域、权威区域、附加区域各自有几条记录

域名解析报文格式

如何解读下面这个DNS报文?

这是一个解析请求还是响应? 里面包含什么内容?

```
▶ Frame 68: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) on interface 0
▶ Ethernet II, Src:                                    , Dst:
▶ Internet Protocol Version 4, Src:            , Dst:
▶ User Datagram Protocol, Src Port: 53, Dst Port: 56693
▼ Domain Name System (response)
    [Request In: 67]
    [Time: 0.010760000 seconds]
    Transaction ID: 0xc3fa
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ www.seu.edu.cn: type A, class IN
  ▼ Answers
    ▶ www.seu.edu.cn: type CNAME, class IN, cname www-seu-edu-cn.cname.saaswaf.com
    ▶ www-seu-edu-cn.cname.saaswaf.com: type CNAME, class IN, cname seu-ipv6.cache.saaswaf.com
    ▶ seu-ipv6.cache.saaswaf.com: type A, class IN, addr 121.194.14.142
  ▶ Additional records
```

中场休息，请回顾：

互联网域名的解析结构是怎样的?

递归域名服务器的功能是什么?

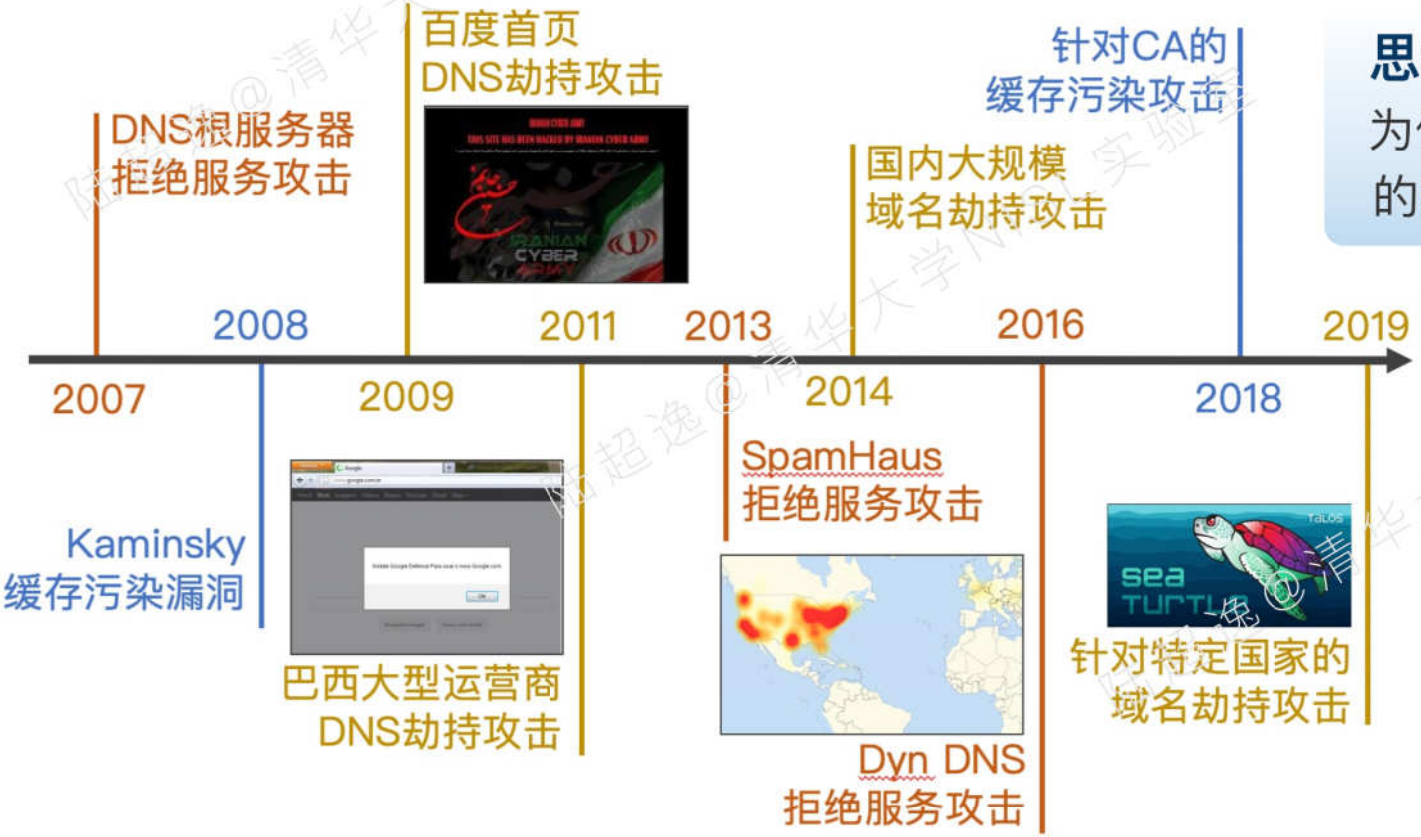
怎样解读域名解析报文?

第二部分 Part II

域名系统的安全威胁

一个事实：域名系统安全事件频发

后果：严重影响互联网的稳定运行



思考：

为什么域名系统安全事件的影响一般都比较大？

域名系统的实现有什么问题?

采用基于UDP协议的明文传输模式

问题	安全风险	典型案例
消息完整性缺失	无法校验响应是否被篡改	中间人域名劫持 旁路注入攻击（缓存污染） 互联网审查
身份认证机制缺失	无法校验解析报文的来源	域名解析路径劫持攻击 恶意域名服务器 拒绝服务攻击（DoS）
消息保密性缺失	解析报文对链路设备可见	用户隐私嗅探

其他方面：域名滥用等

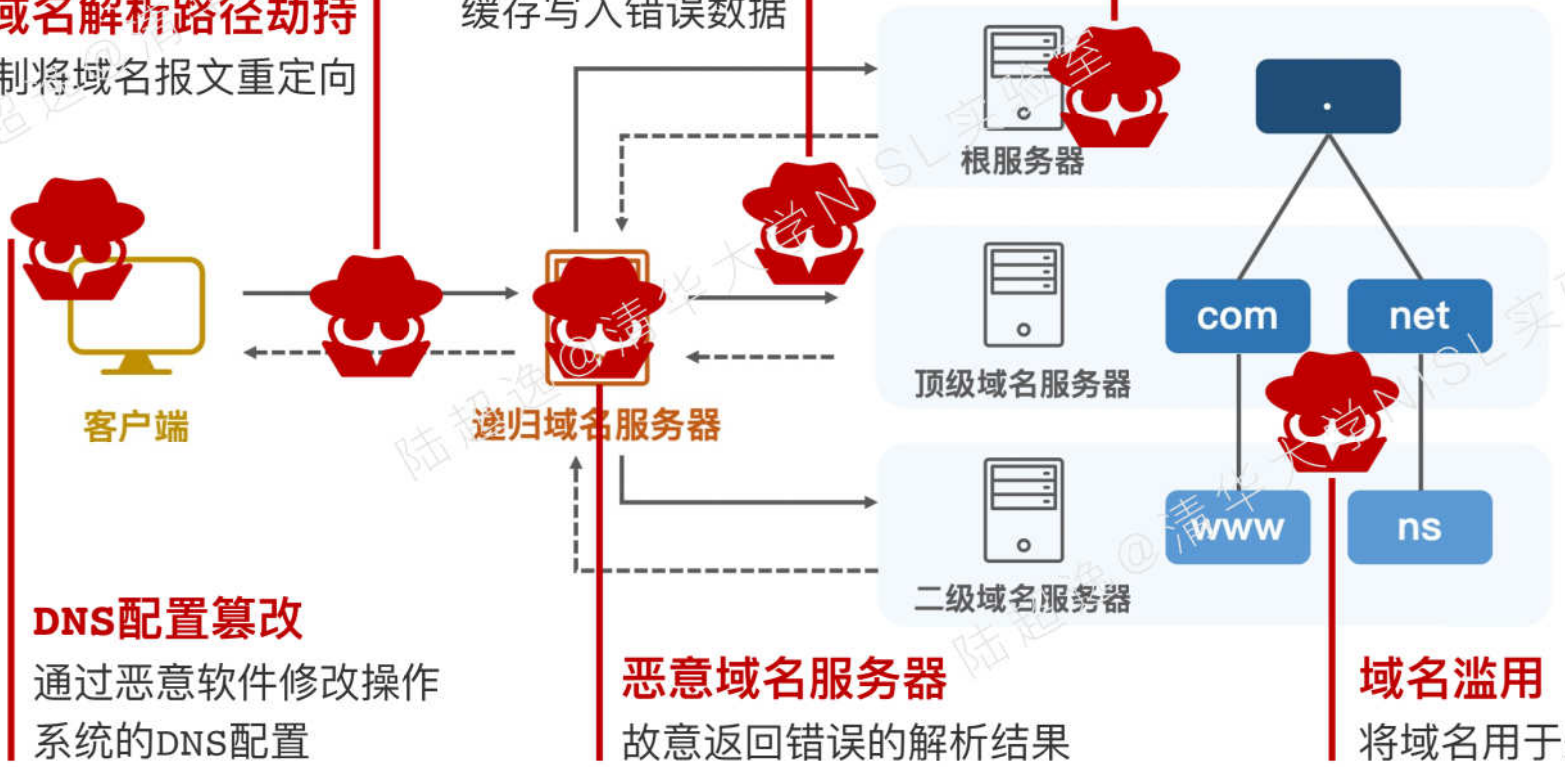
攻击者可能出现在什么位置?

中间人域名劫持
篡改响应报文

域名解析路径劫持
强制将域名报文重定向

缓存污染攻击
向递归域名服务器的
缓存写入错误数据

恶意/虚假权威服务器
非授权的服务器镜像

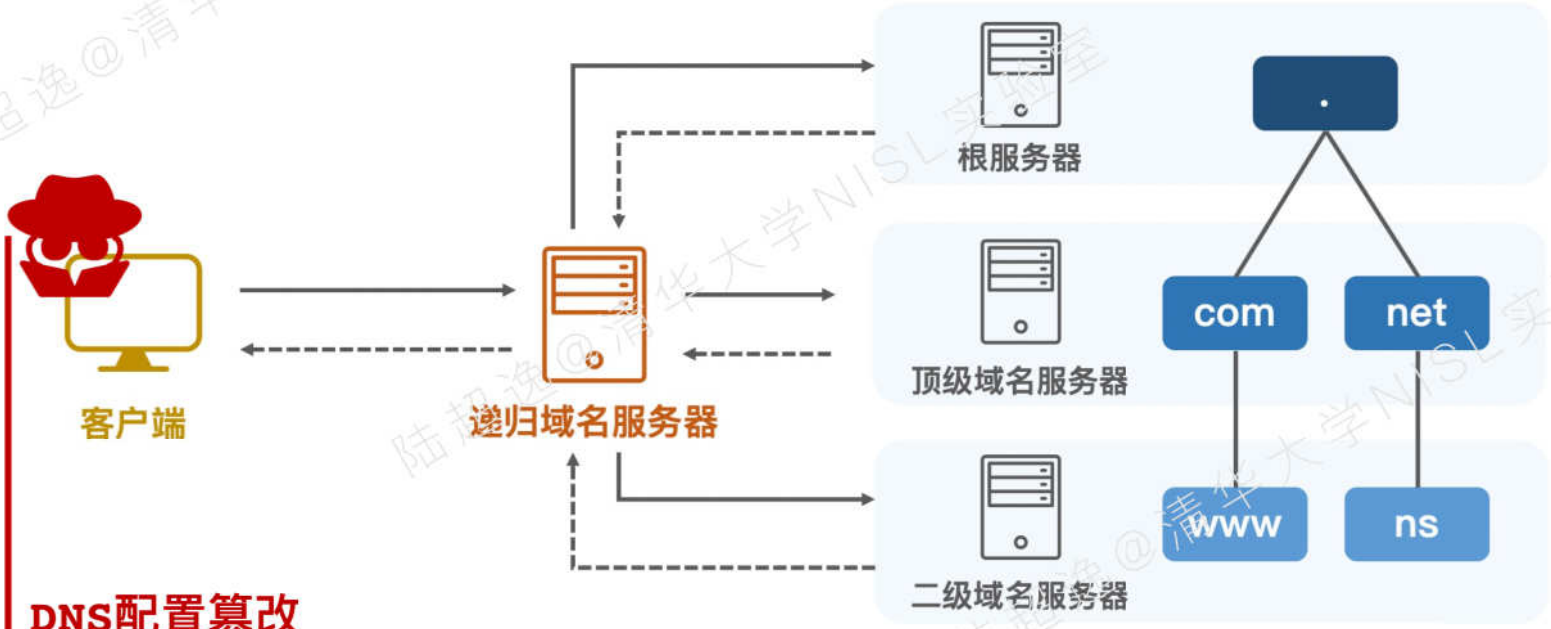


DNS配置篡改
通过恶意软件修改操作
系统的DNS配置

恶意域名服务器
故意返回错误的解析结果

域名滥用
将域名用于恶意行为

攻击者可能出现在什么位置?



DNS配置篡改

通过恶意软件修改操作系统的DNS配置

攻击者可能出现在什么位置?

CNCERT发布关于境内大量家用路由器DNS服务器被篡改情况的通报

2020年06月19日 09:33　作者:　[字号: 大 中 小] 打印

2019年2月19日，CNCERT监测发现，境内部分用户通过家用路由器访问部分网站时被劫持到涉黄涉赌网站。经研判，这是一起典型的由互联网地下黑色产业争斗引发的网络安全事件。具体情况通报如下：

DNS配置篡改

通过恶意软件修改操作系统的DNS配置

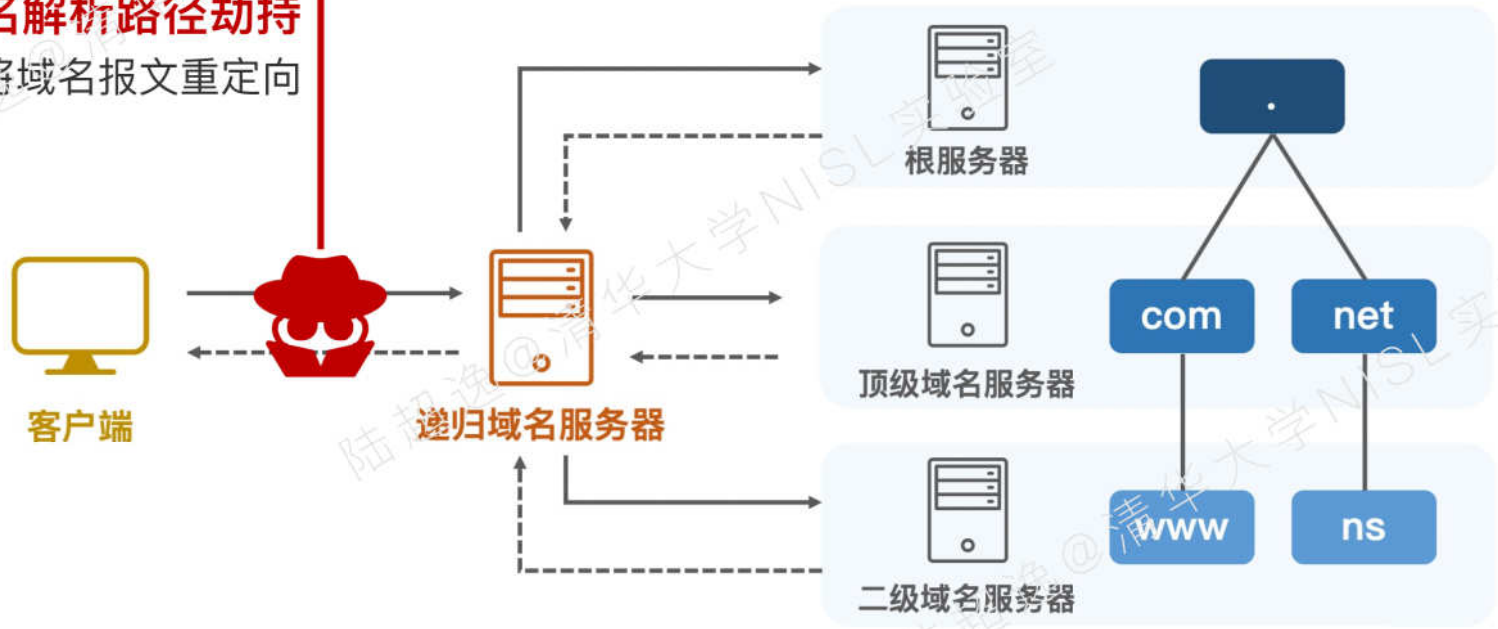
攻击者可能出现在什么位置?

中间人域名劫持

篡改响应报文

域名解析路径劫持

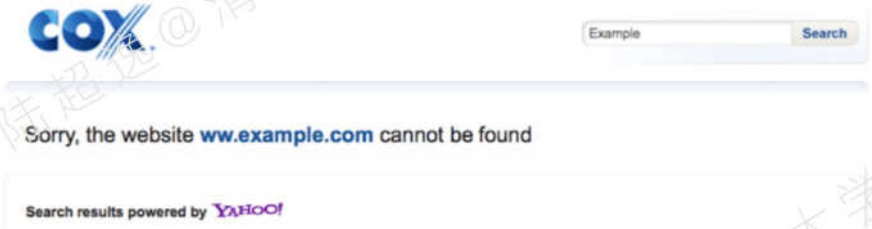
强制将域名报文重定向



解析链路上的劫持篡改

中间人域名劫持案例：流量变现行为

原理：将不存在的域名指向含广告的页面，以赚取利润

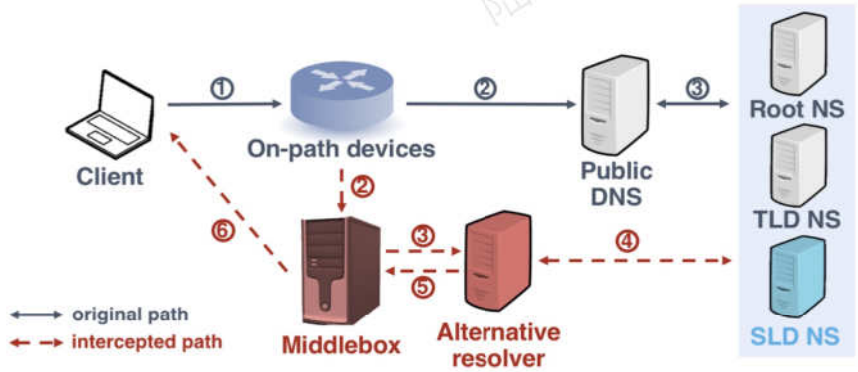


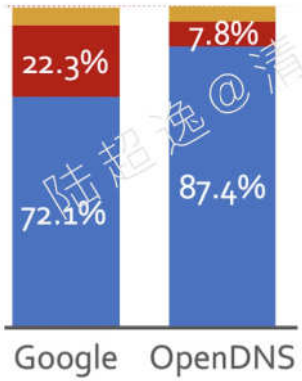
思考：

访问一个不存在的域名，正常情况下应该看到什么？

域名解析路径劫持案例：流量重定向

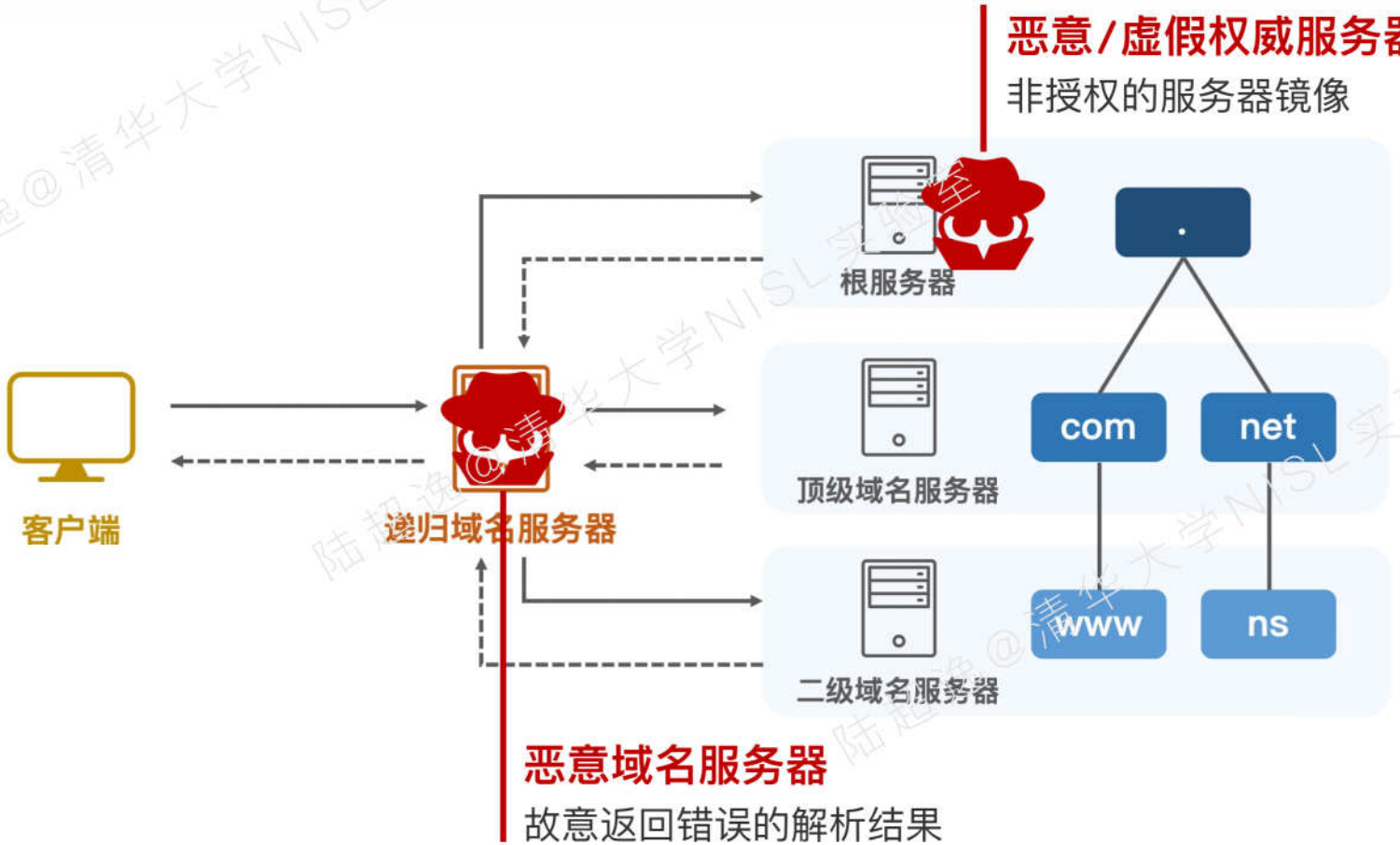
原理：将用户的域名解析流量引至自己的服务器，并伪装成原服务器应答





国内去往Google DNS的查询流量，有1/4被劫持到了其他地方[Liu 18]

攻击者可能出现在什么位置?



不老实的域名服务器

公共递归域名服务器（Open resolver）：谁都可以用的域名解析服务

借助流行的DNS服务软件（如BIND），任何人都可以搭建

IPv4地址空间内，可以通过全网扫描获得

近年来数量逐渐减少，目前量级在**2M左右**

哪些域名最容易被返回错误的解析结果？

赌博、色情、P2P、……

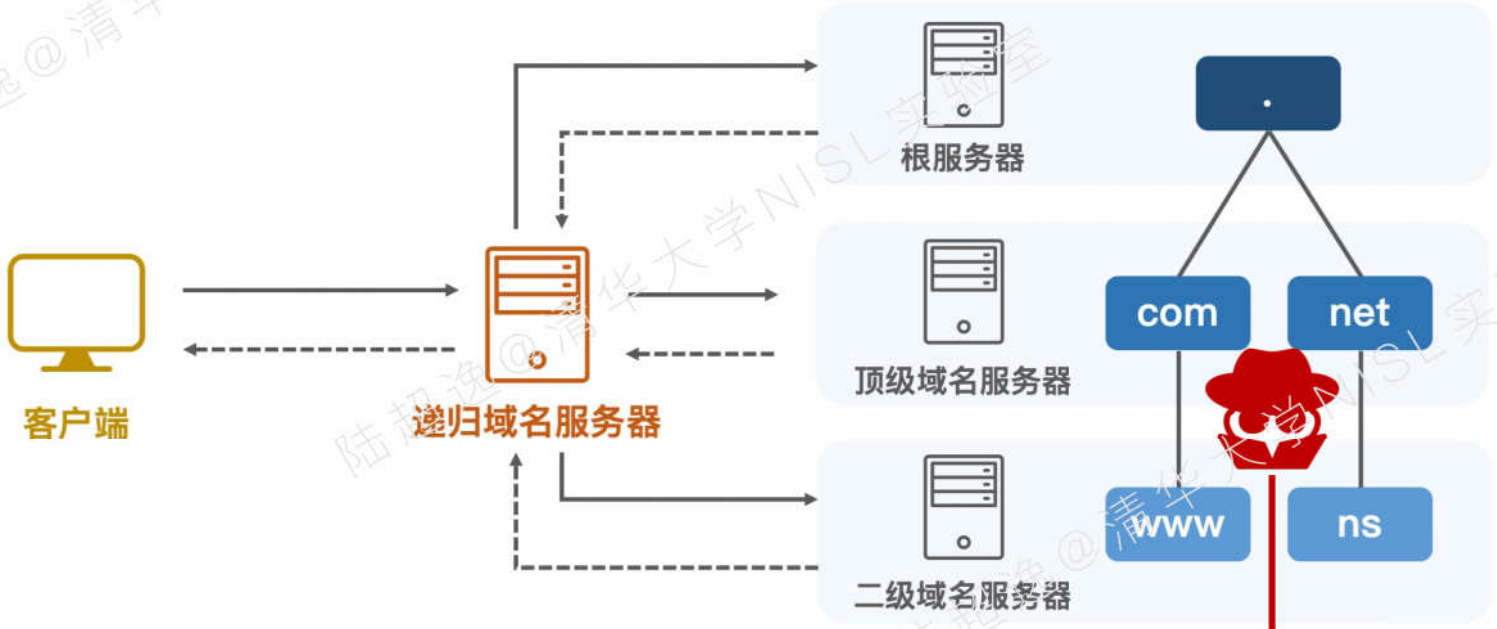
思考：

这个判断解析结果是否正确的实验，应该怎么做？

Rank	Domain Name	Category	# Cn	# Res
1	*pokerstars.com	Gambling	19	251
2	betway.com	Gambling	19	234
3	pornhub.com	Pornography	19	222
4	youporn.com	Pornography	19	192
5	xvideos.com	Pornography	19	174
6	thepiratebay.org	P2P sharing	18	236
7	thepiratebay.se	P2P sharing	18	217
8	xhamster.com	Pornography	18	200
9	*partypoker.com	Gambling	17	226
10	beeg.com	Pornography	17	183
80	torproject.org	Anon. & cen.	12	159
181	twitter.com	Twitter	9	160
250	*youtube.com	Google	8	165
495	*citizenlab.org	Freedom expr.	4	148
606	www.google.com	Google	3	56
1086	google.com	Google	1	5

部分被劫持最多的域名 [Pearce 17]

攻击者可能出现在什么位置?



域名滥用

形似域名抢注（domain squatting）：千奇百怪的“模仿秀”

模仿知名域名，让人傻傻分不清，从而蹭流量

类别	构造规则	域名案例
拼写错误变换	模拟键盘输入错误	youtu**eb**.com（相邻字母交换） y**i**utube.com（键盘位置相邻字母替换）
比特反转变换	字母内部比特反转	youtub**u**.com
添词变换	在知名域名的基础上添加新词	youtube**-videos**.com youtube**customerservice**.com
添级变换	级数大，以知名域名作为前缀	youtube.com.**youtube-new.com**
同形异义	使用不同字符集中的相似字符	y**0**utube.com（使用ASCII字符替换） youtub**ė**.com（使用其他字符替换）

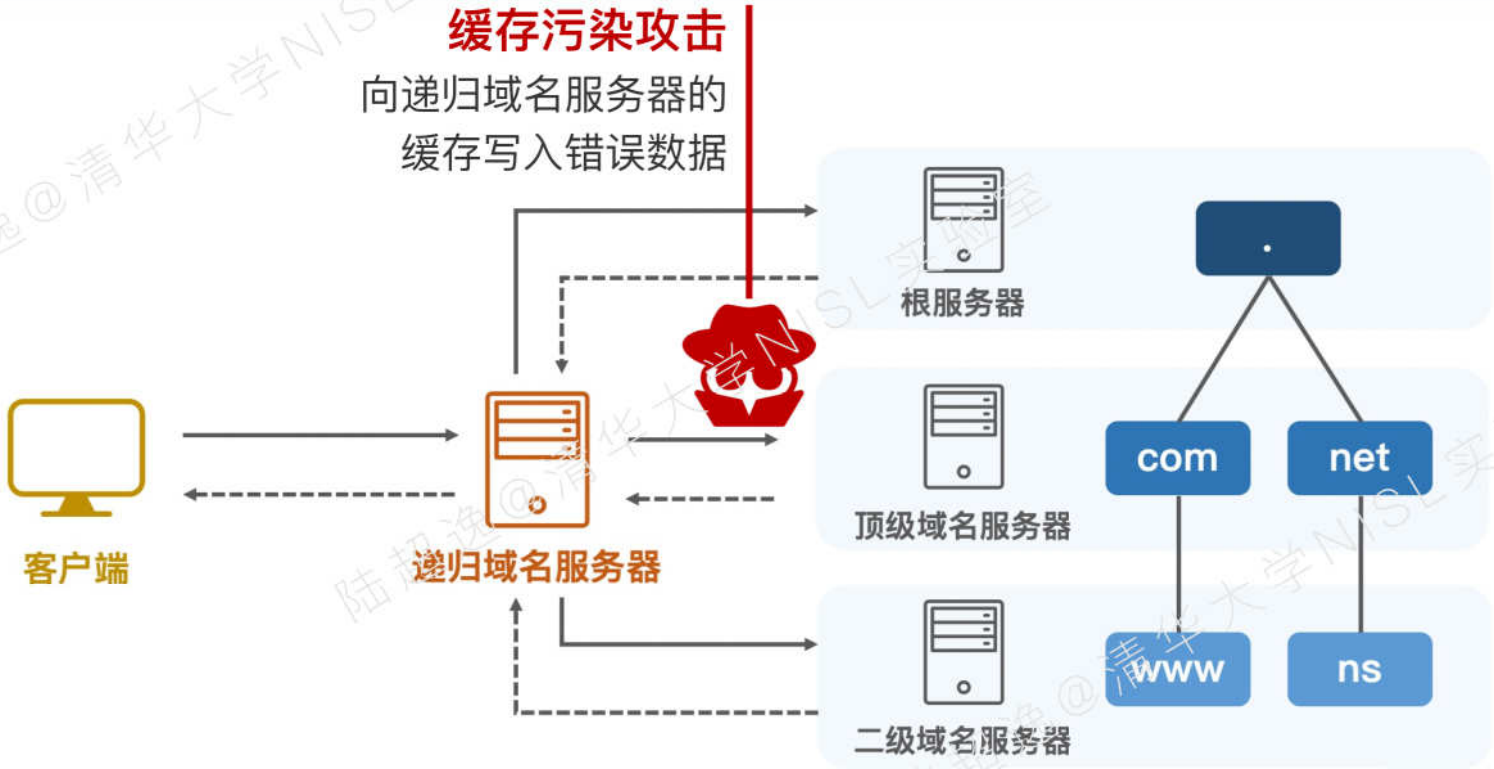
2/3场休息，请回顾：

域名系统安全事件的影响为什么大?

域名系统的脆弱性体现在哪些方面?

域名系统的代表性攻击包括哪些?

攻击者可能出现在什么位置?

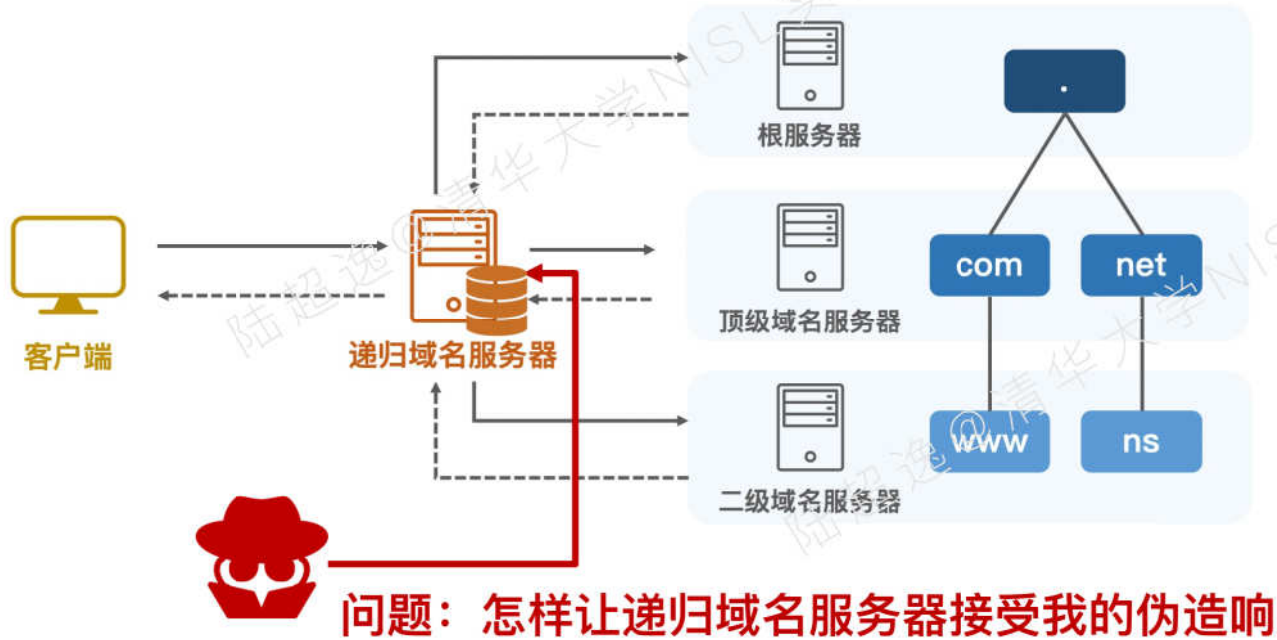


缓存污染攻击

攻击模型：旁路注入（off-path injection）

攻击者**并不位于域名解析链路上**，无法直接嗅探和修改报文

攻击者想要**注入一个伪造的响应**，使得递归域名服务器接受并写入缓存



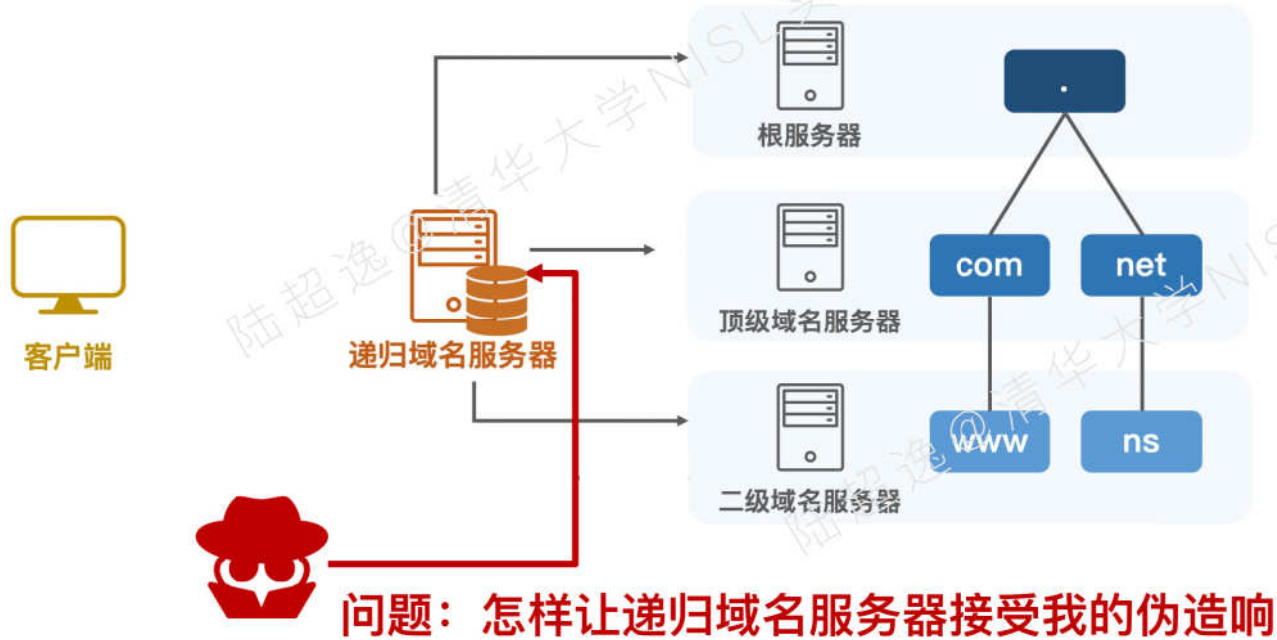
问题：怎样让递归域名服务器接受我的伪造响应?

缓存污染攻击

攻击模型：旁路注入（off-path injection）

攻击者**并不位于域名解析链路上**，无法直接嗅探和修改报文

攻击者想要**注入一个伪造的响应**，使得递归域名服务器接受并写入缓存



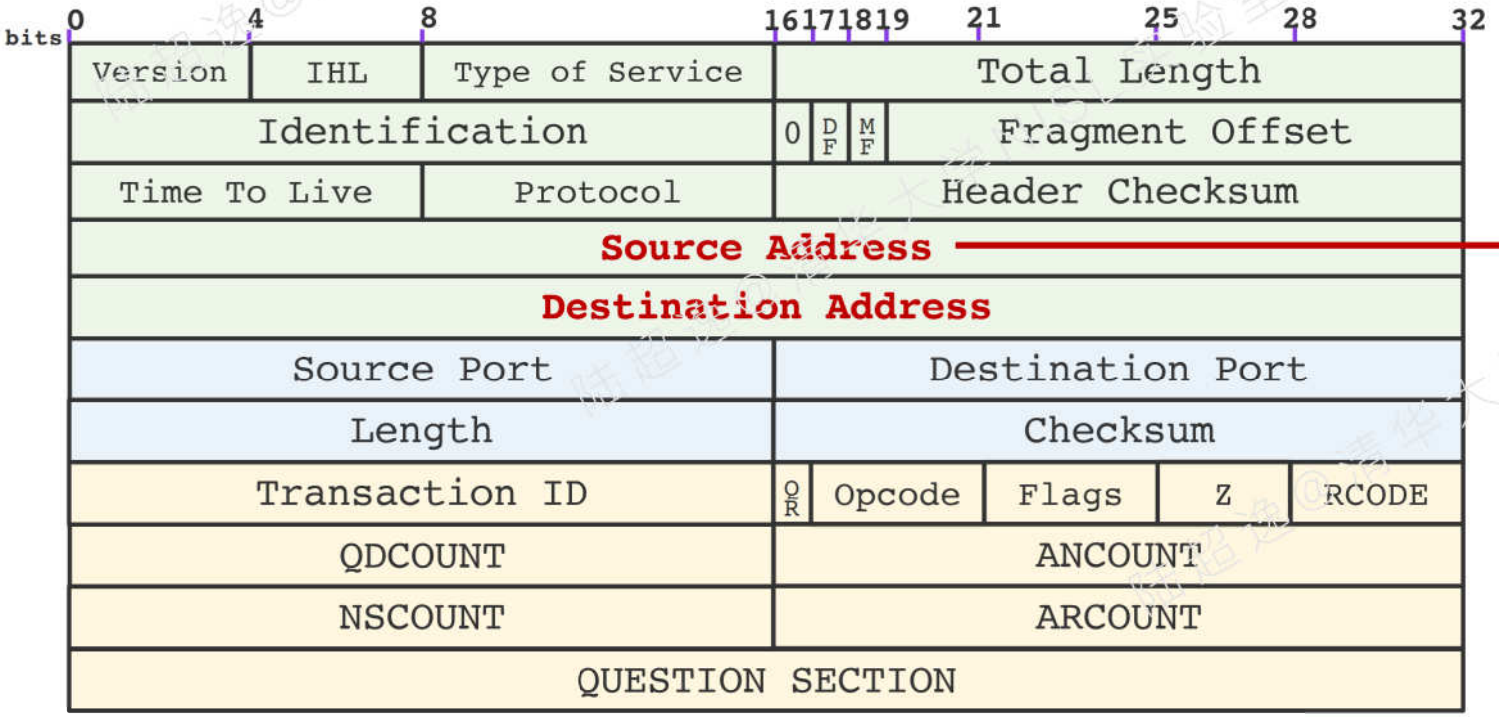
问题：怎样让递归域名服务器接受我的伪造响应?

答案：与递归域名服务器发出的某个请求相匹配!

缓存污染攻击

什么样的响应会被递归域名服务器接收?

递归域名服务器会做什么检查?



1. IP地址匹配

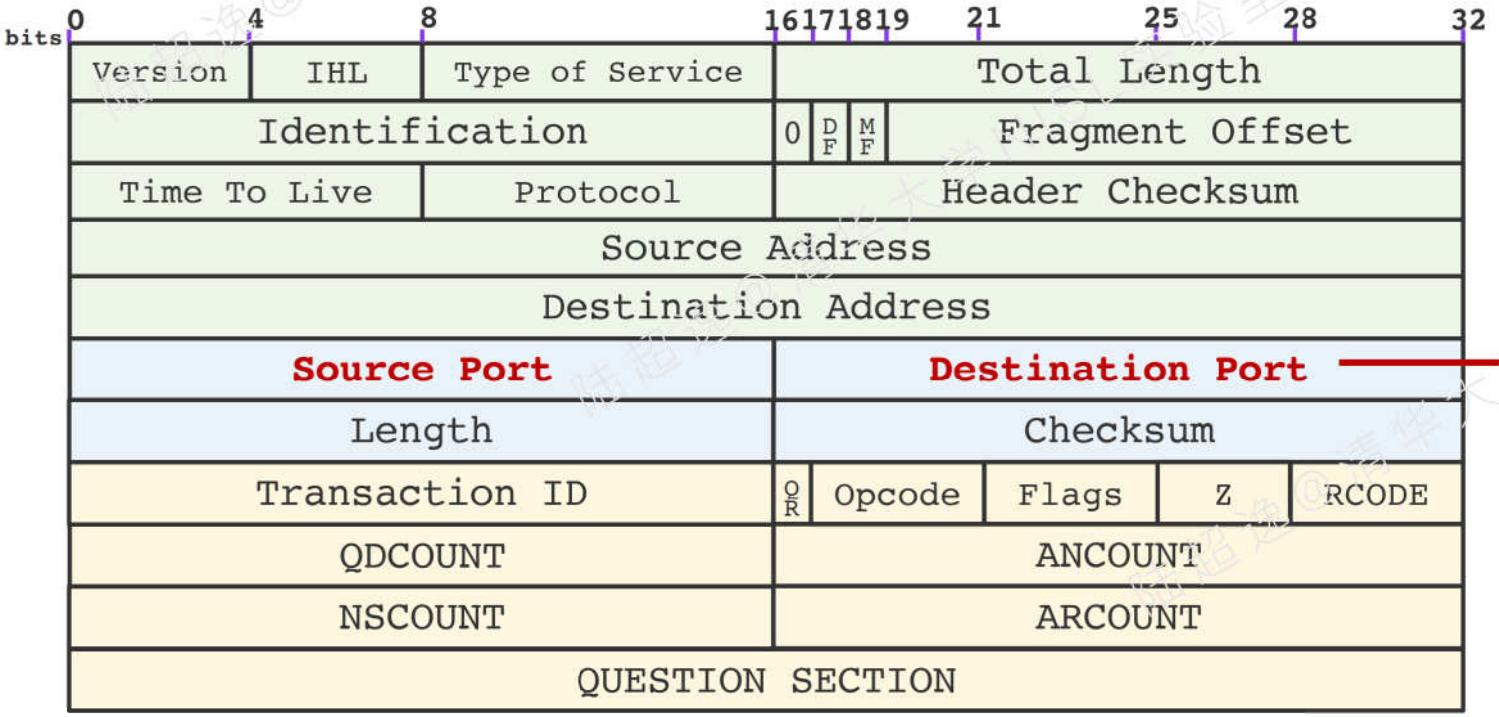
我问的谁

那就应该是谁回答我

缓存污染攻击

什么样的响应会被递归域名服务器接收?

递归域名服务器会做什么检查?



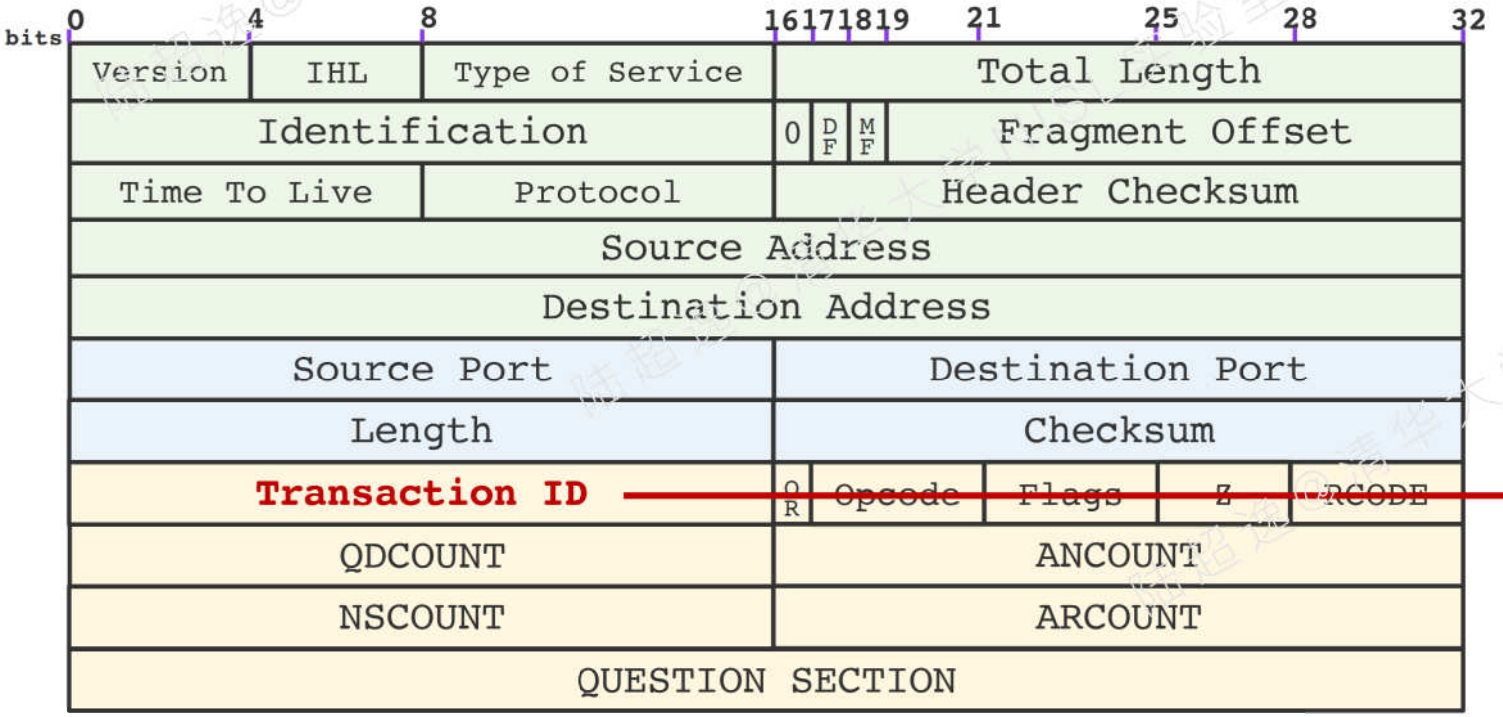
2. 端口匹配

我用哪个端口发请求
那响应就该到这个端口

缓存污染攻击

什么样的响应会被递归域名服务器接收?

递归域名服务器会做什么检查?



3. TXID匹配

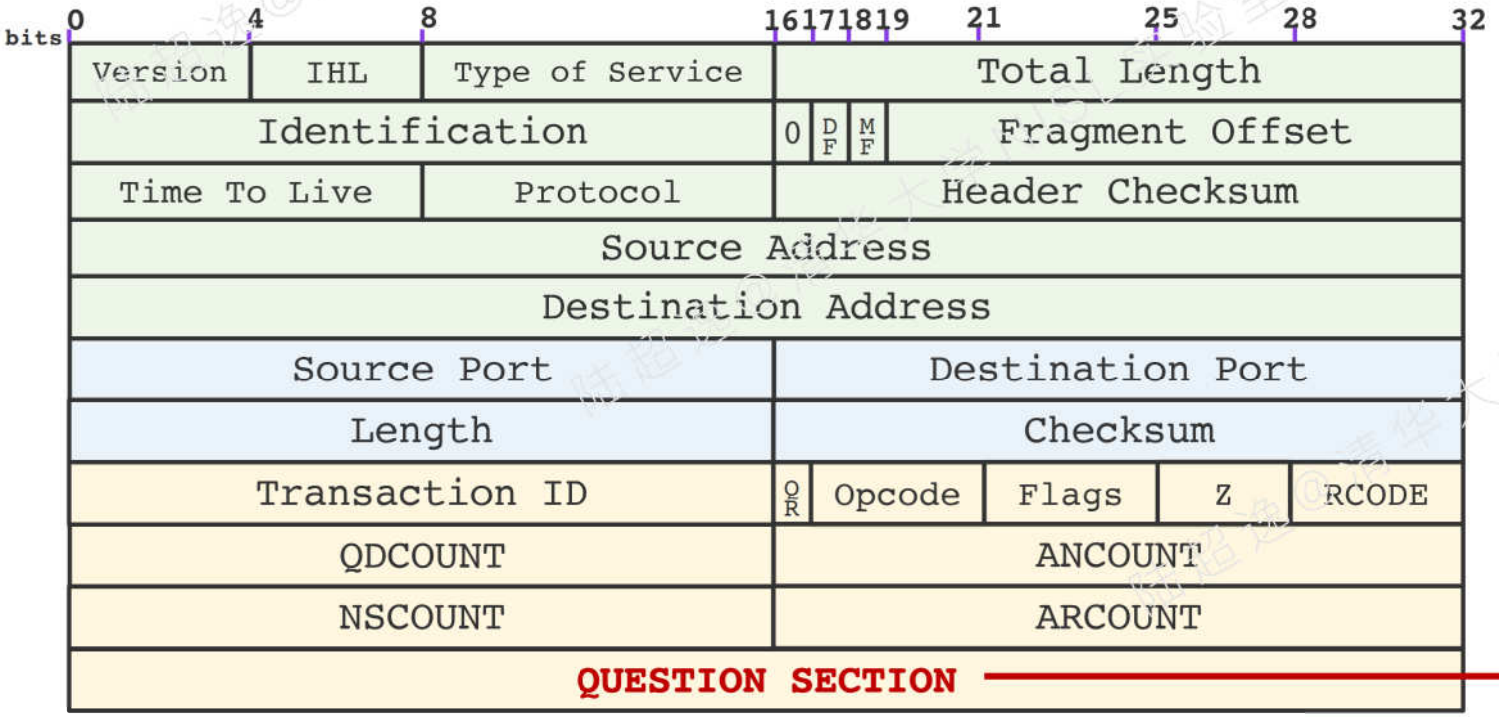
请求是什么值

响应就该是什么值

缓存污染攻击

什么样的响应会被递归域名服务器接收?

递归域名服务器会做什么检查?



4. 问题区域匹配

问你什么你就答什么

缓存污染攻击

攻击者如何伪造符合上述条件的响应?

条件	备注	是否可控/可预知
IP地址匹配	响应源地址 = 权威服务器地址	是（通过查询实现）
	响应目的地址 = 递归域名服务器	是
端口匹配	响应源端口 = 53（DNS默认服务端口）	是
	响应目的端口 = 请求源端口	否
TXID匹配	响应TXID = 请求TXID	否
问题区域匹配	响应问题区域 = 请求问题区域	是（为什么？）
伪造响应先到达	伪造响应先于真实响应到达	是

缓存污染攻击

通过“自问自答”的方式，使得问题区域匹配

需要猜解请求源端口 & 请求TXID

思考：

这样的响应检查机制，提供了多大程度的保护?

5/6场休息，请回顾：

什么是缓存污染攻击?

怎样进行缓存污染攻击?

缓存污染攻击的后果是什么?

第三部分 Part III

域名系统的安全防御

“打补丁”式的安全防御思路

回顾：域名系统的实现有什么问题?

缺什么，我们就加什么

问题	安全风险	典型案例
消息完整性缺失	无法校验响应是否被篡改	中间人域名劫持 旁路注入攻击（缓存污染） 互联网审查
身份认证机制缺失	无法校验解析报文的来源	域名解析路径劫持攻击 恶意域名服务器 拒绝服务攻击（DoS）
消息保密性缺失	解析报文对链路设备可见	用户隐私嗅探

“打补丁”式的安全防御思路

回顾：域名系统的实现有什么问题?

缺什么，我们就加什么

问题	解决方案
消息完整性缺失	域名签名协议（DNSSEC） 对响应中的资源记录进行**数字签名和验证**
身份认证机制缺失	加密域名协议（Encrypted DNS） 使用**加密信道**传输域名解析报文，基于证书进行身份认证
消息保密性缺失	

域名签名协议（DNSSEC）

数字签名（Digital signature）：发送方签名、接收方验证

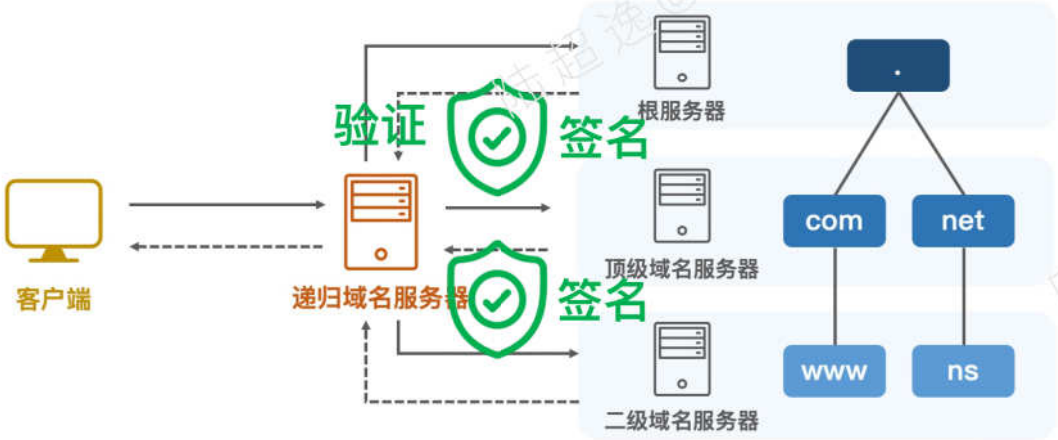
发送方使用**私钥签名**、公开公钥，接收方使用**公钥验证**

私钥只有发送方拥有 -> 数字签名无法伪造

DNSSEC的工作位置

域名所有者（权威服务器）：**生成各资源记录（集）的数字签名**，塞进响应报文中

递归域名服务器：使用公钥**验证响应报文中的数字签名**



思考：

DNSSEC能够防御什么攻击？

域名签名协议（DNSSEC）

练习：如何解读DNSSEC报文?

```
▼ Domain Name System (query)
    [Response In: 80]
    Transaction ID: 0x032c
  ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ paypal.com: type A, class IN
  ▼ Additional records
    ▼ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▼ Z: 0x8000
          1... .... .... .... = DO bit: Accepts DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
```

观察：

这两个报文多出来了什么东西?

```
▼ Domain Name System (response)
    [Request In: 78]
    [Time: 0.091791000 seconds]
    Transaction ID: 0x032c
  ▶ Flags: 0x81a0 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ paypal.com: type A, class IN
  ▼ Answers
    ▼ paypal.com: type A, class IN, addr 64.4.250.36
        Name: paypal.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 72
        Data length: 4
        Address: 64.4.250.36
    ▶ paypal.com: type A, class IN, addr 64.4.250.37
    ▼ paypal.com: type RRSIG, class IN
        Name: paypal.com
        Type: RRSIG (46)
        Class: IN (0x0001)
        Time to live: 72
        Data length: 158
        Type Covered: A (Host Address) (1)
        Algorithm: RSA/SHA1 (5)
        Labels: 2
        Original TTL: 300 (5 minutes)
        Signature Expiration: Aug 14, 2022 20:05:36.000000000 CST
        Signature Inception: Jul 15, 2022 19:34:50.000000000 CST
        Key Tag: 11811
        Signer's name: paypal.com
        Signature: 6d00ab5e2bda2b1c63d27db831279897538385e2cc6fb9d4...
```

加密域名协议

基于UDP协议的明文传输 -> 基于加密信道的传输

在DNS协议下方**直接“套上”TLS等加密传输协议**

加密信道建立前，基于**数字证书**认证服务器身份

加密DNS协议的工作位置

客户端至递归域名服务器之间

思考：

加密DNS协议能够防御什么攻击？

加密DNS和DNSSEC是否可以结合使用？

理论授课结束，请回顾：

域名系统的安全增强包含哪些?

DNSSEC的原理是什么？工作位置在哪里?

加密DNS协议的原理是什么？工作位置在哪里?