

第一章问题

1.1) A → R:

$$t_{\text{PROP}} = \frac{4\text{km}}{2 \times 10^8 \text{m/s}} = 0.02 \text{ms}$$

$$t_{\text{TRANSP}} = \frac{10000 \text{byte}}{100 \text{Mbps}} = 0.8 \text{ms}$$

R → B: $t_{\text{PROP}} = \frac{2\text{km}}{2 \times 10^8 \text{m/s}} = 0.01 \text{ms}$

$$t_{\text{TRANSP}} = \frac{10000 \text{byte}}{10 \text{Mbps}} = 8 \text{ms}$$

$$\therefore t_{\text{总}} = 8.83 \text{ms}$$

2) 每个组报文长度为 2000 byte

在 A → R 上 $t_{\text{TRANSP}} = 0.8/5 = 0.16 \text{ms}$

在 R → B 上 $t_{\text{TRANSP}}' = 8/5 = 1.6 \text{ms}$

$$\therefore t_{\text{总}} = 0.02 + 0.01 + 0.16 + 8 = 8.19 \text{ms}$$

3) 最主要的影响还是报文长度、链路长度和带宽

在统计多路复用机制中, 其他主机的发送量也会影响时延

报文分组到达时, 如果出口链路忙, 则报文分组需要在路由器缓存中排队等待, 引入排队时延, 排队时延对网络性能影响较大。

第二章问题

1)

通过使用Windows命令行模式提供的nslookup命令查询www.baidu.com的IP地址, 给出结果截图, 并对返回的结果进行解释。同时, 利用Wireshark捕获查询的交互过程, 给出结果截图, 并进行简要说明。

```

C:\Users\26937>nslookup www.baidu.com
服务器:  UnKnown
Address:  222.30.45.41

非权威应答:
名称:     www.a.shifen.com
Addresses: 39.156.66.14
          39.156.66.18
Aliases:  www.baidu.com

C:\Users\26937>

```

服务器: 因为在查询时并未指定, 所以这里是本机的DNS服务器的名称

Adderss: 222.30.45.41, 是本机的DNS IP地址, 可以用ipconfig作为佐证

```

C:\WINDOWS\system32\cmd.exe

TCP/IP 上的 NetBIOS . . . . . : 已启用
fec0:0:0:ffff::3%1

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Qualcomm QCA9377 802.11ac Wireless Adapter
   物理地址. . . . . : 28-CD-C4-3E-77-63
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址 . . . . . : 2001:250:401:6562:dec4:e3f4:3e4a:3d2(首选)
   临时 IPv6 地址. . . . . : 2001:250:401:6562:9da6:a007:d10:4d2(首选)
   本地链接 IPv6 地址. . . . . : fe80::7888:ac10:727a:6158%2(首选)
   IPv4 地址 . . . . . : 10.130.82.49(首选)
   子网掩码 . . . . . : 255.255.128.0
   获得租约的时间 . . . . . : 2022年11月22日 20:32:42
   租约过期的时间 . . . . . : 2022年11月23日 2:35:44
   默认网关. . . . . : fe80::865b:12ff:fe5e:3603%2
                        10.130.0.1
   DHCP 服务器 . . . . . : 10.130.0.1
   DHCPv6 IAID . . . . . : 36228548
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-BB-C0-9D-C0-3E-BA-34-D4-08
   DNS 服务器 . . . . . : 222.30.45.41
                        202.113.18.41
TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 蓝牙网络连接:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

```

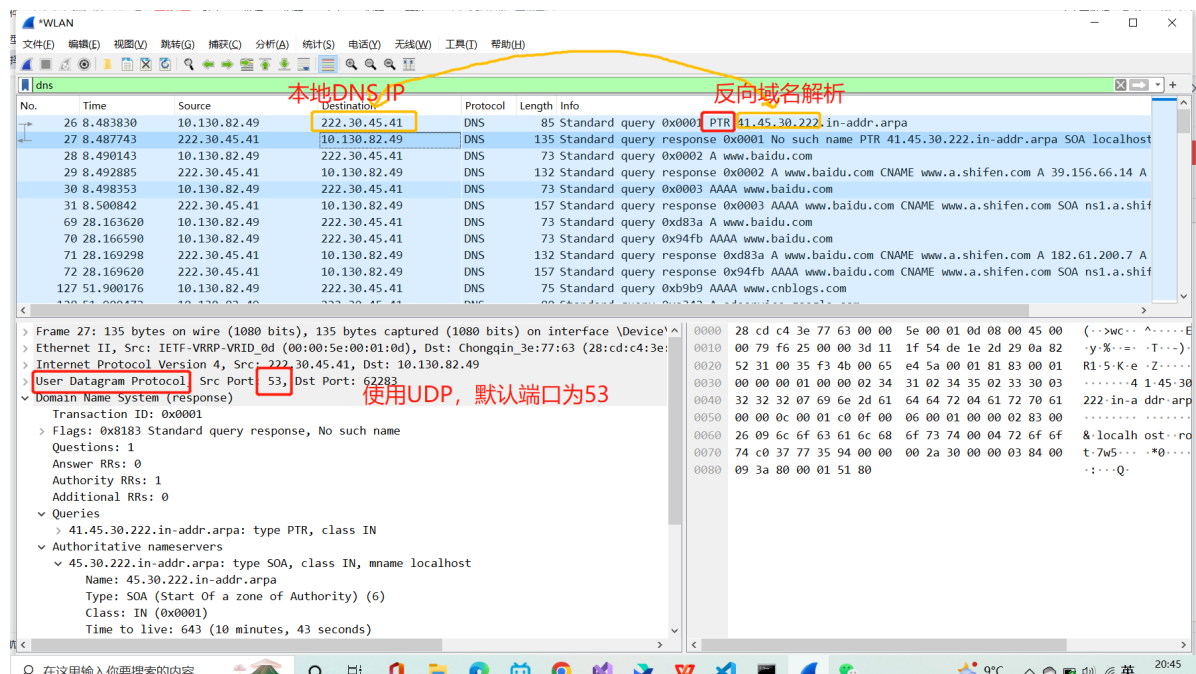
非权威应答: 代表这里得到的ip地址并不是去访问权威的百度DNS服务器得到的, 而是在其他服务器上缓存的

名称: 代表了name, 百度用的name是www.a.shifen.com

Addresses:是百度的ip地址, 有多个ip

aliases: 别名, 所以用www.baidu.com也可以进行访问

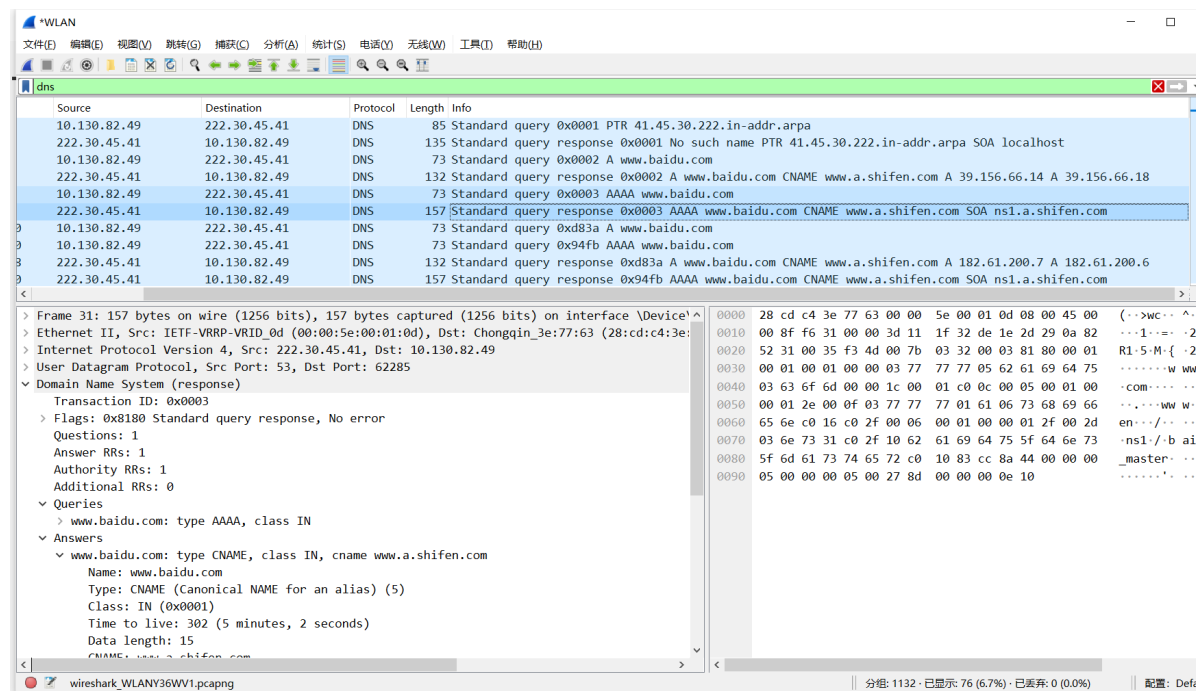
wireshark捕获



本机ip地址为10.130.82.49，可以看到本机地址发出了多个query请求，

先向DNS服务器发出query，利用PTR进行反向解析，根据信息中的41.45.30.222可以看到网络通讯协议与本机CPU字节序使用的段模式不同，x86是小端模式，网络字节序是大端模式，返回信息 SOA描述负责区域的域名服务器、版本信息，为localhost，代表是本地

之后本地DNS查询对应的ipv4 (A) 和ipv6 (AAAA) 地址，事物ID分别为0x0002和0x0003



ipv4查询，返回别名和ipv4地址， ipv6查询返回别名和SOA，这里的ns1.a.shifen.com是权威百度DNS服务器，可以看到报文格式里包含了

- 事务 ID (Transaction ID)：DNS 报文的 ID 标识。对于请求报文和其对应的应答报文，该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。
- 标志 (Flags)：DNS 报文中的标志字段。
- 问题计数 (Questions)：DNS 查询请求的数目。
- 回答资源记录数 (Answers RRs)：DNS 响应的数目。
- 权威名称服务器计数 (Authority RRs)：权威名称服务器的数目。
- 附加资源记录数 (Additional RRs)：额外的记录数目 (权威名称服务器对应 IP 地址的数目)。

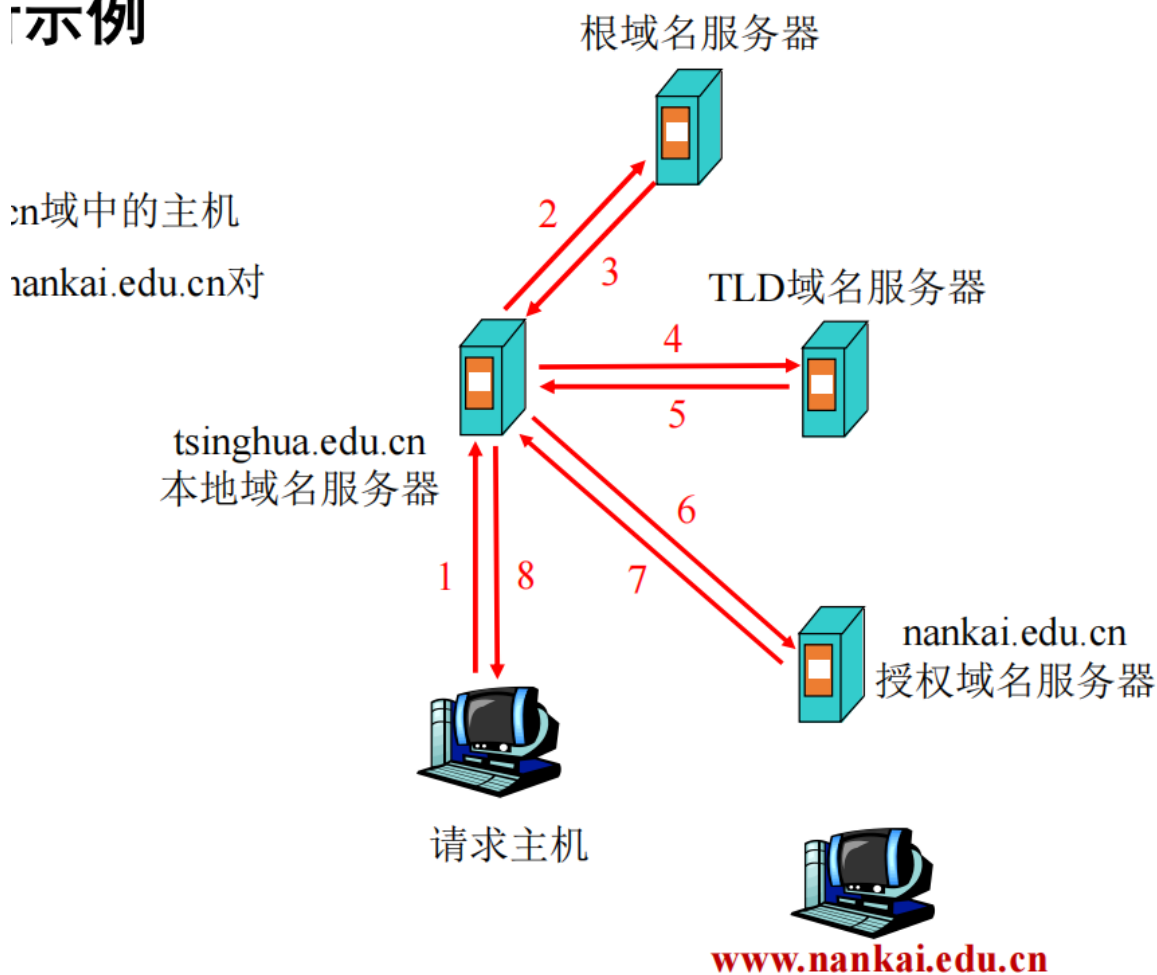
answer字段里

- Name: DNS 请求的域名。
- Type: 资源记录的类型，与问题部分中的查询类型值是一样的。
- Class: 地址类型，与问题部分中的查询类值是一样的。
- Time to live: 生存时间，以秒为单位，表示资源记录的生命周期，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。它同时也可以表明该资源记录的稳定程度，稳定的信息会被分配一个很大的值。
- Data length: 资源数据的长度。
- 资源数据: 表示按查询段要求返回的相关资源记录的数据。（如 Address :IP地址，CNAME:服务器别名，等）

2)

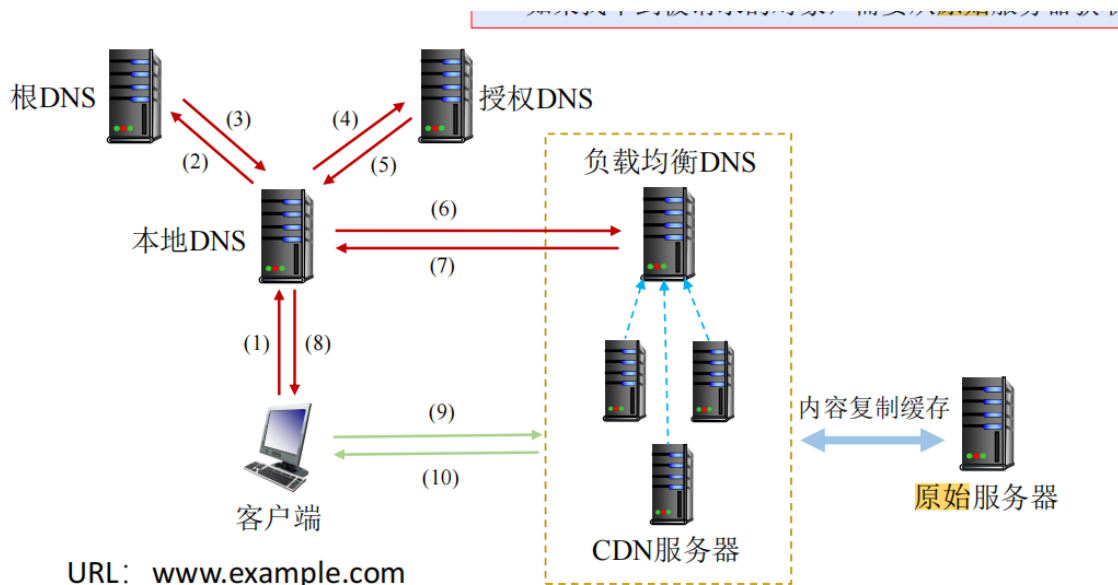
以反复解析为例，说明域名解析的基本工作过程（可以结合图例）。给出内容分发网络（CDN）中DNS重定向的基本方法，说明原始资源记录应该如何修改，并描述重定向过程。

示例



上图是tsinghua.edu.cn域中的主机要解析www.nankai.edu.cn对应的IP地址，请求主机先向本地域名服务器发送请求，然后本地域名服务器向根域名服务器发送请求，当根域名服务器收到本地域名服务器发出的查询请求报文时，要么给出所要查询的IP地址，要么告诉本地服务器：“你下一步应当向哪一个域名服务器进行查询”。然后让本地服务器进行后续的查询。在上图中，根域名服务器把自己知道的顶级域名服务器的IP地址告诉本地域名服务器，让本地域名服务器再向顶级域名服务器查询。顶级域名服务器在收到本地域名服务器的查询请求后，要么给出所要查询的IP地址，要么告诉本地服务器下一步应当向哪一个权威域名服务器进行查询。上图中，顶级域名服务器告诉本地服务器要查询的授权域名服务器

nankai.edu.cn，然后进行查询，得到了所要解析的IP地址，然后把这个结果返回给发起查询的主机。由于有缓存机制，其实有时候反复解析查询不用如此复杂，可能会返回某个服务器中缓存的数据。



没有CDN时，域名解析会执行上述策略，但是有了域名解析之后，如果想要解析权威域名，就不会直接访问该权威域名，而是通过负载均衡DNS，负载均衡DNS会为用户选择一台合适的缓存服务器提供服务，选择的依据包括：

- 1) 根据用户 IP 地址，判断哪一台服务器距用户最近；
- 2) 用户所处的运营商；
- 3) 根据用户所请求的 URL 中携带的内容名称，判断哪一台服务器上用户所需的内容；
- 4) 查询各个服务器当前的负载情况，判断哪一台服务器尚有服务能力。

原始资源应该部分复制缓存在CDN服务器中，并保留缓存记录，这样负载均衡DNS才可以进行判断。

3)

在DNS域名系统中，域名解析时使用UDP协议提供的传输层服务（DNS服务器使用UDP的53端口），而UDP提供的是不可靠的传输层服务，请你解释DNS协议应如何保证可靠机制？

DNS协议关于UDP和TCP的选择通常为以下两种情况：

- (1) 若DNS客户程序事先知道响应报文的长度大于512B，则应当使用TCP连接；

主域名服务器与辅助域名服务器在进行区域传送时，通常数据量都比较大，所有DNS规定，区域传送使用TCP协议。

(2) 若解析程序不知道响应报文的长度，它一般使用UDP协议发送DNS查询报文，若DNS响应报文的长度大于512B，服务器就截断响应报文，在这种情况下，DNS客户程序通常使用TCP重发原来的查询请求，从而它将来能够从DNS服务器中收到完整的响应。