



南开大学
Nankai University

书面作业一

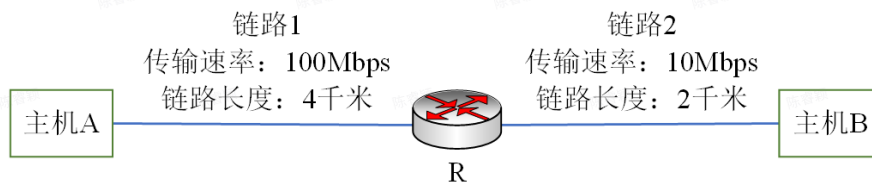
- 姓名：陈睿颖
- 学号：2013544
- 专业：计算机科学与技术

1. 第一章问题

网络结构如下图所示，主机A与主机B之间通过两段链路和一台转发设备R进行连接，每条链路的长度和传输速率已经在图中标出，R采用存储转发机制。主机A向主机B发送一个长度为10000字节的报文，请回答以下问题（设电磁波传播速度为 2×10^8 米/秒）

1. 如果采用报文交换，请计算端到端的最小时延，即从主机A传输报文的第一位开始，到主机B接收到报文的最后一位为止所用的时间。
2. 如果将报文分成5个报文分组传输，请计算完成报文传输的最小端到端时延（忽略报文分组的封装开销）。

在统计多路复用机制中，端到端的时延具有不确定性，请简要分析影响端到端时延的主要因素。



1) 共有2个链路



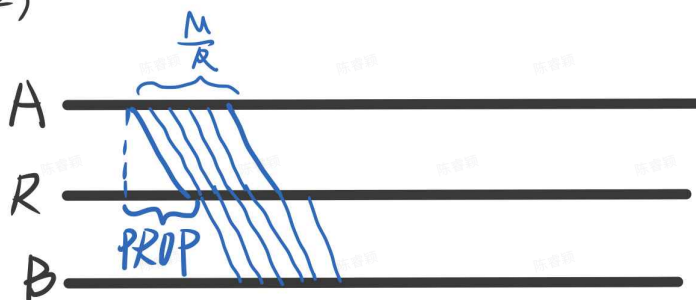
$$TRANSP_1 = \frac{P}{R_1} = \frac{10000 \times 8}{10^8} = 8 \times 10^{-4} s$$

$$PROP_1 = \frac{L_1}{C} = \frac{4 \times 10^3}{2 \times 10^8} = 2 \times 10^{-5} s$$

$$TRANSP_2 = \frac{P}{R_2} = \frac{8 \times 10^4}{10^7} = 8 \times 10^{-3} s$$

$$PROP_2 = \frac{L_2}{C} = \frac{2 \times 10^3}{2 \times 10^8} = 10^{-5} s \quad \text{总时间为 } 8.83 \times 10^{-3} s = 8.83 ms$$

12)



$$T = PROP_1 + PROP_2 + \frac{M}{R_2} + \frac{M}{5R_1} = 3 \times 10^{-5} + \frac{8}{5} \times 10^{-4} + 8 \times 10^{-3} = 8.19 \times 10^{-3} s = 8.19 ms$$

2. 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。

如图所示，在Windows中用nslookup命令采用直接查询的方法的结果：

```
C:\WINDOWS\system32>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: 182.61.200.7
          182.61.200.6
Aliases: www.baidu.com
```

- address表示的是DNS服务器地址
- 名称代表显示的是百度原来的网址
- 剩下的Addresses是百度的IP地址
- Aliaes代表目标域名

查询到www.baidu.com的IP地址为182.61.200.7、182.61.200.6;

利用wireshark捕获上述过程的交互过程如下:

No.	Time	Source	Destination	Protocol	Length	Info
24	5.596120	10.130.10.144	222.30.45.41	DNS	72	Standard query 0x24eb AAAA www.bing.com
25	5.597853	222.30.45.41	10.130.10.144	DNS	277	Standard query response 0x24eb AAAA www.bing.com CNAME www-www.bing.com.trafficmanager.net CNL...
89	11.129175	10.130.10.144	222.30.45.41	DNS	85	Standard query 0x0001 PTR 41.45.30.222.in-addr.arpa
90	11.131095	222.30.45.41	10.130.10.144	DNS	135	Standard query response 0x0001 No such name PTR 41.45.30.222.in-addr.arpa SOA localhost
91	11.132887	10.130.10.144	222.30.45.41	DNS	73	Standard query 0x0002 A www.baidu.com
92	11.134297	222.30.45.41	10.130.10.144	DNS	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.com A 182.61.200.6 A 182.61...
93	11.136835	10.130.10.144	222.30.45.41	DNS	73	Standard query 0x0003 AAAA www.baidu.com
94	11.138101	222.30.45.41	10.130.10.144	DNS	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com
133	16.867878	10.130.10.144	222.30.45.41	DNS	73	Standard query 0x830f AAAA www.baidu.com
134	16.869811	222.30.45.41	10.130.10.144	DNS	157	Standard query response 0x830f AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com
153	16.928386	10.130.10.144	222.30.45.41	DNS	82	Standard query 0x0cad A az700632.vo.msecnd.net
154	16.929809	222.30.45.41	10.130.10.144	DNS	193	Standard query response 0x0cad A az700632.vo.msecnd.net CNAME az700632-pme.azureedge.net CNAML...
155	16.929953	10.130.10.144	222.30.45.41	DNS	82	Standard query 0xc8c3 AAAA az700632.vo.msecnd.net
156	16.931376	222.30.45.41	10.130.10.144	DNS	205	Standard query response 0xc8c3 AAAA az700632.vo.msecnd.net CNAME az700632-pme.azureedge.net C...

91号数据包是DNS请求报文, 92号数据是DNS响应报文。

对91号数据包进行分析:

这里我们展开了Domain Name System节点。客户端向服务器发送DNS查询报文, 这是一个标准查询 (Standard Query), 我们可以理解为正向解析。

> Frame 91: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF...

> Ethernet II, Src: IntelCor_dc:4a:9c (0c:7a:15:dc:4a:9c), Dst: IETF-VRRP-VRID_0d (00:00:5e:00:00:0d)

> Internet Protocol Version 4, Src: 10.130.10.144, Dst: 222.30.45.41

> User Datagram Protocol, Src Port: 50784, Dst Port: 53

> Domain Name System (query)

Transaction ID: 0x0002

Flags: 0x0100 Standard query

0... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

.... 0... .. = Truncated: Message is not truncated

.... 1... .. = Recursion desired: Do query recursively

.... 0... .. = Z: reserved (0)

.... 0... .. = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

> Queries

[Response In: 92]

0000 00 00 5e 00 01 0d 0c 7a 15 dc 4a 9c 08 00 45 00 ..^...z...J...E-

0010 00 3b d7 5e 00 00 08 11 00 00 0a 82 0a 90 de 1e .;.^.....

0020 2d 29 c6 60 00 35 00 27 20 92 00 02 01 00 00 01 -).^5..

0030 00 00 00 00 00 00 03 77 77 77 05 62 61 69 64 75w ww·baidu

0040 03 63 6f 6d 00 00 01 00 01com.....

查询报文分为首部和问题两个部分。首部包含ID，标志和计数器3类字段。Opcode值为0表示标准查询。Question为1表示只有1个查询报文，其他3个资源记录数均为0。问题部分给出了要查询的域名、类型、和类。这个报文封装在UDP协议上，发往DNS服务器，传输的目的端口号为53号。

对92号数据进行分析：

> User Datagram Protocol, Src Port: 53, Dst Port: 50784

▼ Domain Name System (response)

Transaction ID: 0x0002

Flags: 0x8180 Standard query response, No error

1... .. = Response: Message is a response

.000 0... .. = Opcode: Standard query (0)

... .0... .. = Authoritative: Server is not an authority for domain

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query recursively

... ..1... .. = Recursion available: Server can do recursive queries

... ..0... .. = Z: reserved (0)

... ..0... .. = Answer authenticated: Answer/authority portion was not authentic

... ..0... .. = Non-authenticated data: Unacceptable

... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

[Request In: 91]

[Time: 0.001410000 seconds]

0000	0c 7a 15 dc 4a 9c 00 00	5e 00 01 0d 08 00 45 00	z...J...^....E..
0010	00 76 ae dc 00 00 3d 11	ae 41 de 1e 2d 29 0a 82	-v....=-.A.--)..
0020	0a 90 00 35 c6 60 00 62	06 68 00 02 81 80 00 01	...5..`b.h.....
0030	00 03 00 00 00 00 03 77	77 77 05 62 61 69 64 75w ww.baidu
0040	03 63 6f 6d 00 00 01 00	01 c0 c0 00 05 00 01 00	...com.....
0050	00 00 e3 00 0f 03 77 77	77 01 61 06 73 68 69 66ww w.a.shif
0060	65 6e c0 16 c0 2b 00 01	00 01 00 00 00 e4 00 04	en++++.....
0070	b6 3d c8 06 c0 2b 00 01	00 01 00 00 00 e4 00 04	==...+...
0080	b6 3d c8 07		==..

这里我们展开了Domain Name System节点。服务器返回客户端DNS应答报文。应答报文分为首部、问题、回答、权威、附加5个部分。首部包含ID，标志和计数器3类字段。ID与查询报文相同。Question为1表示只有一个查询报文，其他3个资源记录数给出了相应的数目，问题部分与查询部分相同。

▼ Answers

▼ www.baidu.com: type CNAME, class IN, cname www.a.shifen.com

Name: www.baidu.com

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 227 (3 minutes, 47 seconds)

Data length: 15

CNAME: www.a.shifen.com

▼ www.a.shifen.com: type A, class IN, addr 182.61.200.6

Name: www.a.shifen.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 228 (3 minutes, 48 seconds)

Data length: 4

Address: 182.61.200.6

▼ www.a.shifen.com: type A, class IN, addr 182.61.200.7

Name: www.a.shifen.com

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 228 (3 minutes, 48 seconds)

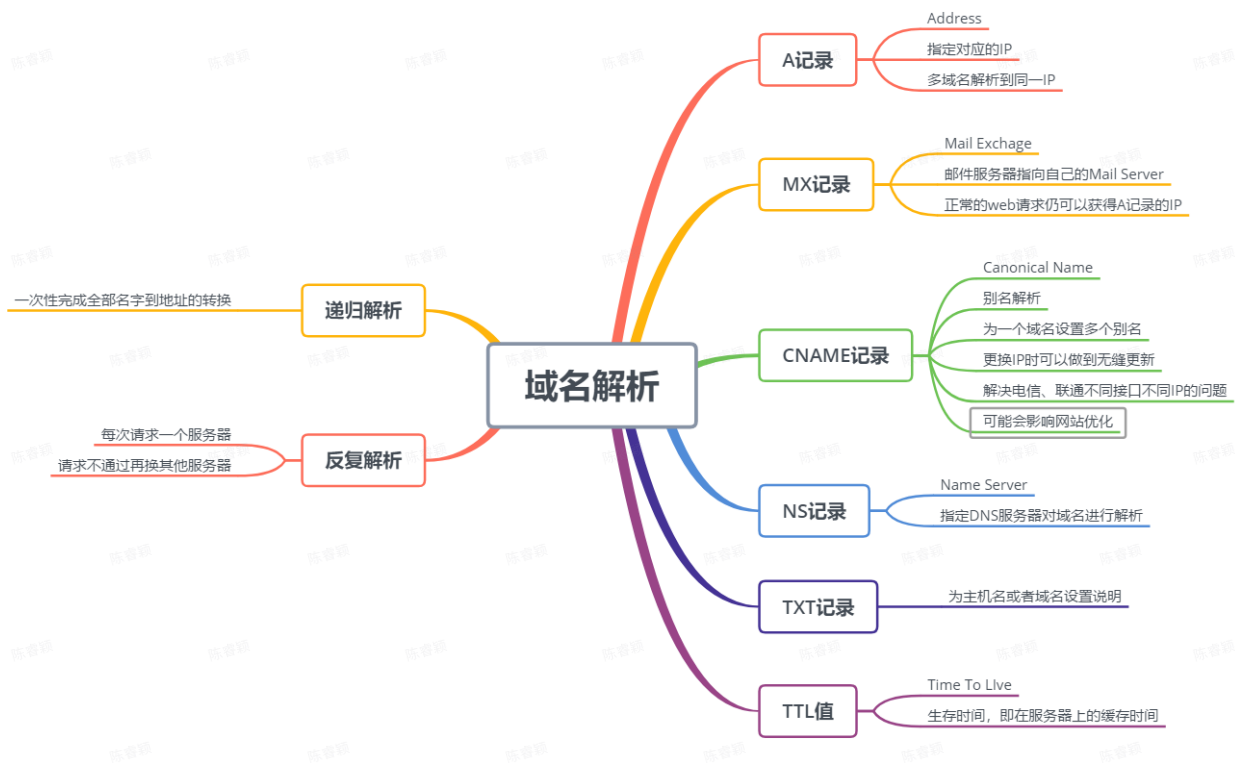
Data length: 4

Address: 182.61.200.7

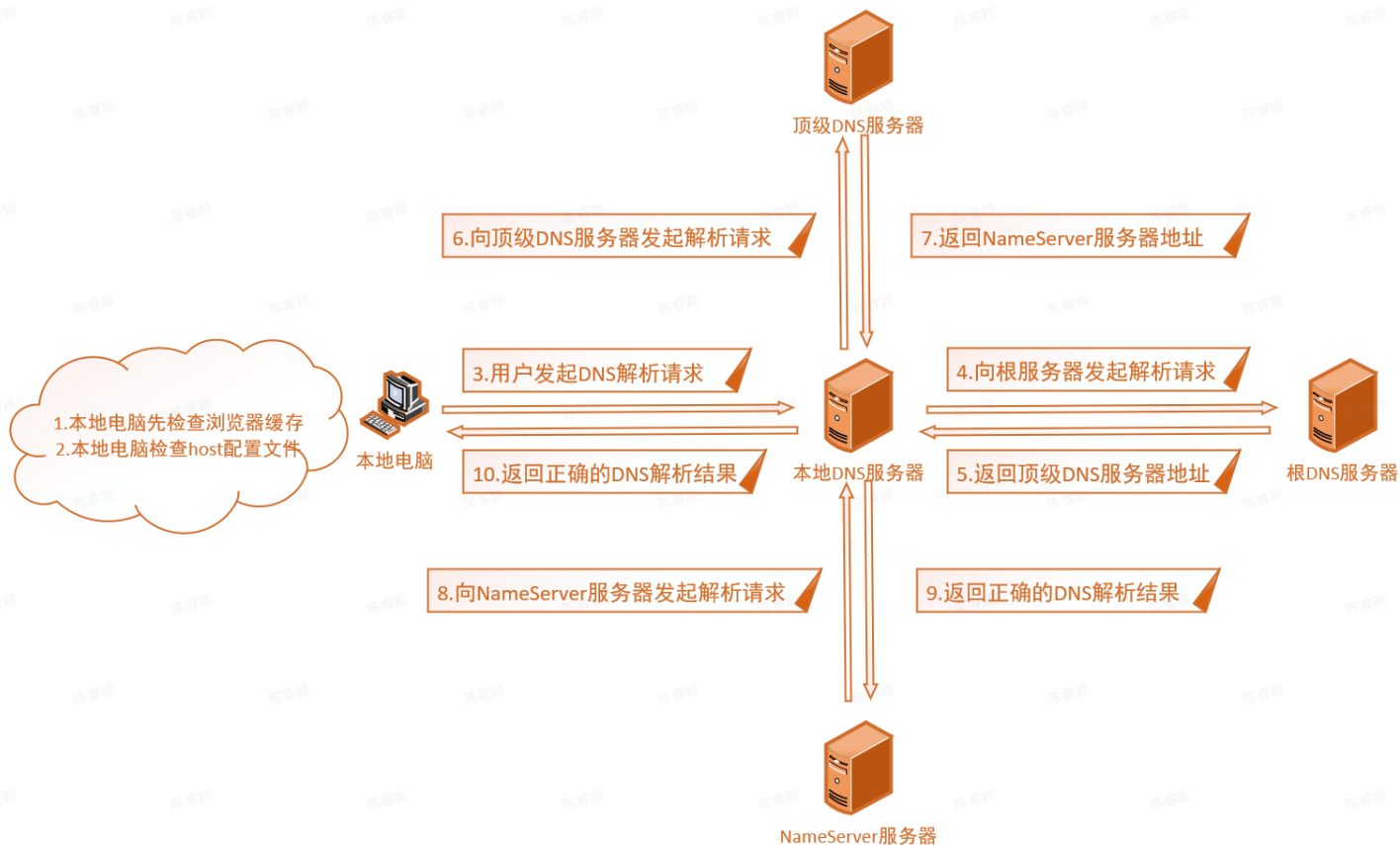
在展开Answers节点。每条记录都包括名称、类型、类、生存时间、数据长度和数据6个字段

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。

反复解析指每次请求一个服务器，如果不通再请求别的服务器。



以www.baidu.com为例，主要通过图中10个步骤进行域名解析



具体分析如下：

- 1.本地电脑会检查浏览器缓存中有没有这个域名对应的解析过的IP地址，如果缓存中有，这个解析过程就结束。浏览器缓存域名也是有限制的，不仅浏览器缓存大小有限制，而且缓存的时间也有限制，通常情况下为几分钟到几小时不等，域名被缓存的时间限制可以通过TTL属性来设置。这个缓存时间太长和太短都不太好，如果时间太长，一旦域名被解析到的IP有变化，会导致被客户端缓存的域名无法解析到变化后的IP地址，以致该域名不能正常解析，这段时间内有一部分用户无法访问网站。如果设置时间太短，会导致用户每次访问网站都要重新解析一次域名。
- 2.如果浏览器缓存中没有数据，浏览器会查找操作系统缓存中是否有这个域名对应的DNS解析结果。其实操作系统也有一个域名解析的过程，在Linux中可以通过/etc/hosts文件来设置，而在windows中可以通过配置C:\Windows\System32\drivers\etc\hosts文件来设置，用户可以将任何域名解析到任何能够访问的IP地址。例如，我们在测试时可以将一个域名解析到一台测试服务器上，这样不用修改任何代码就能测试到单独服务器上的代码的业务逻辑是否正确。正是因为有这种本地DNS解析的规程，所以有黑客就可能通过修改用户的域名来把特定的域名解析到他指定的IP地址上，导致这些域名被劫持。
- 3.如果浏览器缓存中没有数据，浏览器会查找操作系统缓存中是否有这个域名对应的DNS解析结果。其实操作系统也有一个域名解析的过程，在Linux中可以通过/etc/hosts文件来设置，而在windows中可以通过配置C:\Windows\System32\drivers\etc\hosts文件来设置，用户可以将任何域名解析到任何能够访问的IP地址。例如，我们在测试时可以将一个域名解析到一台测试服务器上，这样不用修改任何代码就能测试到单独服务器上的代码的业务逻辑是否正确。正是因为有这种本地DNS解析的规程，所以有黑客就可能通过修改用户的域名来把特定的域名解析到他指定的IP地址上，导致这些域名被劫持。
- 4.如果本地DNS服务器仍然没有命中，就直接到根DNS服务器请求解析
- 5.根DNS服务器返回给本地DNS域名服务器一个顶级DNS服务器地址，它是国际顶级域名服务器，如.com、.cn、.org等，全球只有13台左右。
- 6.本地DNS服务器再向上一步获得的顶级DNS服务器发送解析请求。
- 7.接受请求的顶级DNS服务器查找并返回此域名对应的Name Server域名服务器的地址，这个Name Server服务器就是要访问的网站域名提供商的服务器，其实该域名的解析任务就是由域名提供商的服务器来完成。比如要访问www.baidu.com，而这个域名是从某公司注册获得的，那么该公司上的服务器就会有www.baidu.com的相关信息。
- 8.接受请求的顶级DNS服务器查找并返回此域名对应的Name Server域名服务器的地址，这个Name Server服务器就是我要访问的网站域名提供商的服务器，其实该域名的解析任务就是由域名提供商的服务器来完成。比如访问www.baidu.com，而这个域名是从A公司注册获得的，那么A公司上的服务器就会有www.baidu.com的相关信息。
- 9.返回该域名对应的IP和TTL值，本地DNS服务器会缓存这个域名和IP的对应关系，缓存时间由TTL值控制。
- 10.把解析的结果返回给本地电脑，本地电脑根据TTL值缓存在本地系统缓存中，域名解析过程结束在实际的DNS解析过程中，可能还不止这10步，如Name Server可能有很多级，或者有一个GTM来负载均衡控制，这都有可能影响域名解析过程。

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。

- 因为UDP提供的是不可靠的传输服务，所以域名解析时的可靠性则要由应用层保障。而在DNS应用层，其报文格式中包括了question和answer的数量，可以用来进行一定的校验。返回的报文中，也包含着发送过去的问题，可以对匹配程度进行一定的比较。报文中还包含了**DNS响应的数目、权威名称服务器数目以及权威名称服务器对应IP地址的数目**，这些条目，也可以进行一定的校验。
- 同时，DNS报文还有**以秒为单位的生存周期**，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。当**生存周期过期后，会重新请求更新，以保证数据的正确性**。
- DNS协议还会**通过冗余设置，避免单点失效**。具体来说，多个为保证高可用性，会有多台权威服务器冗余支持每个区域。某个区域的资源记录通过手动或自动方式更新到单个主权威服务器上，其它冗余名称服务器用作同一区域中主服务器的备份服务器，以防主服务器无法访问或宕机。辅 DNS 服务器定期与主 DNS 服务器通讯，确保它的区域信息保持最新。

综上所述，若本机请求的IP发生错误，则会链接不上网址，发出再次请求，进行正确更新。而高层的DNS服务器则是通过冗余性和定期更新来保证可靠机制。基本上来说，只要高层DNS服务器保证了正确性，就不会发生较大的错误。