

第二章作业

学号: 2011165 姓名: 李欣 专业: 计算机科学与技术

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 $C=2 \times 10^8$ 米/秒)

知识点:

网络核心: 传输时延

■ 报文长度 P : 单位 “位(bit)”

■ 链路长度 L : 单位 “米”

■ 传输速率 R : 单位 “位/秒”

■ 传播时延 $PROP$: 电磁波在介质上传播的时间, 单位 “秒”

$$PROP = L/C, \text{ 其中 } C \text{ 为电磁波传播速度}$$

■ 传输时间 $TRANSP$: 发送长度为 P 的报文所用的时间

$$TRANSP = P/R, \text{ 其中 } R \text{ 为传输速率}$$

■ 端端时延 $Latency$: 发送端开始传送第一位到接收端接收到最后一位所用的时间, 在 **单一链路** 上计算方法为:

$$Latency = PROP + TRANSP$$

链路 1:

传输速率 $R_1=100\text{Mbps}=1 \times 10^8 \text{bit/s}$

链路长度 $L_1=4000\text{m}$

链路 2:

传输速率 $R_2=10\text{Mbps}=1 \times 10^7 \text{bit/s}$

链路长度 $L_2=2000\text{m}$

报文长度 $=P=10000 \text{ 字节}=80000 \text{bit}$

- (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。

解答: 如下图所示为报文交换的过程图

Road1: 链路 1

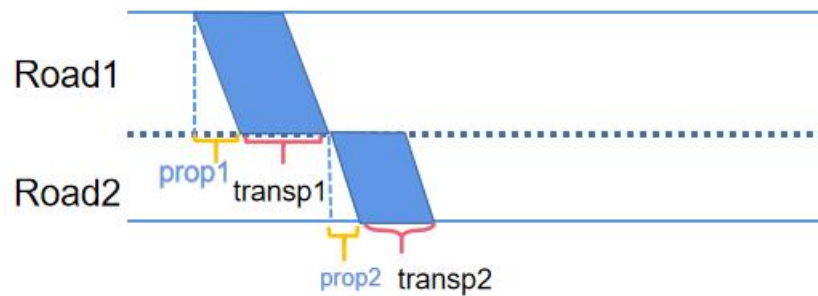
prop1: 链路 1 上的传播时延

transp1: 链路 1 上的传输时间

Road2: 链路 2

prop2: 链路 2 上的传播时延

transp2: 链路 2 上的传输时间



$$\text{prop}_1 = \frac{L_1}{c} = 4000\text{m} / (2 \times 10^8)\text{m/s} = 2 \times 10^{-5} = 0.02 \times 10^{-3}\text{s}$$

$$\text{transp}_1 = \frac{P}{R_1} = 80000\text{bit} / 10^8\text{bit/s} = 8 \times 10^{-4} = 0.8 \times 10^{-3}\text{s}$$

$$\text{prop}_2 = \frac{L_2}{c} = 2000\text{m} / (2 \times 10^8)\text{m/s} = 1 \times 10^{-5} = 0.01 \times 10^{-3}\text{s}$$

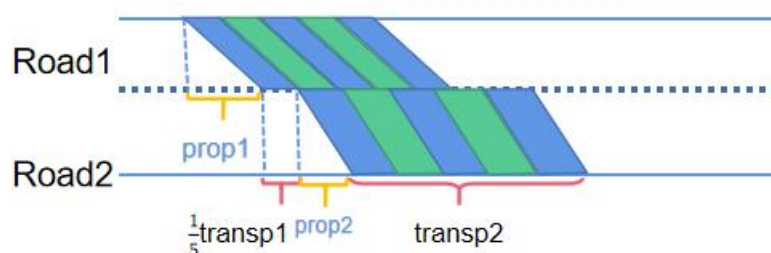
$$\text{transp}_2 = \frac{P}{R_2} = 80000\text{bit} / 10^7\text{bit/s} = 8 \times 10^{-3}\text{s}$$

$$\text{latency} = \text{prop}_1 + \frac{1}{5} \text{transp}_1 + \text{prop}_2 + \text{transp}_2 = (0.02 + 0.8 + 0.01 + 8) \times 10^{-3}\text{s} = 8.83 \times 10^{-3}\text{s}$$

$$= 8.83(\text{ms})$$

(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）。

解答：在第一问中，我们知道了 $\text{transp}_1 < \text{transp}_2$ ，所以不会出现第一个分组在 Road2 上传输完毕但第二个分组还在 Road1 上传输的情况，即 Road2 上的第 $k(0 \leq k \leq 4)$ 个分组传输完毕后立刻传输下一个分组。



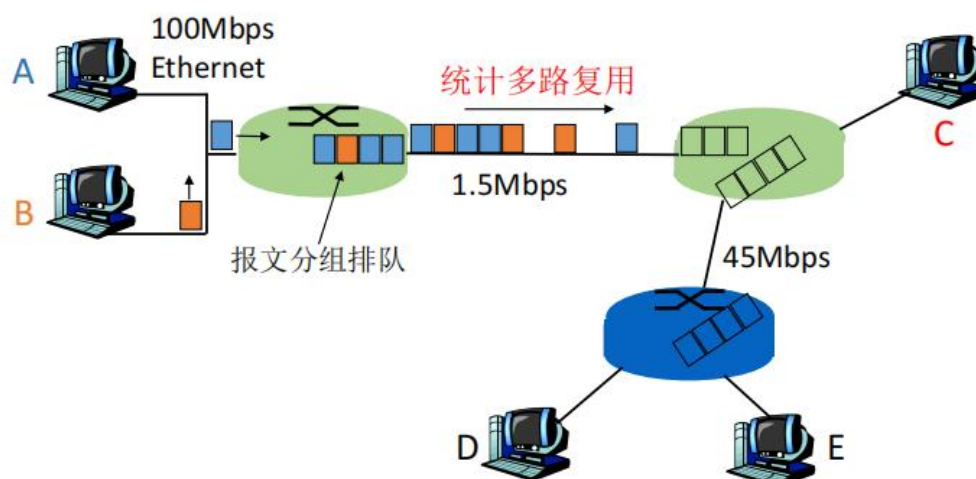
$$\text{latency} = \text{prop}_1 + \frac{1}{5} \text{transp}_1 + \text{prop}_2 + \text{transp}_2 = (0.02 + 0.16 + 0.01 + 8) \times 10^{-3}\text{s} = 8.18 \times 10^{-3}\text{s}$$

= 8.19(ms)

- (3) 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。

知识点：

网络核心：报文分组交换



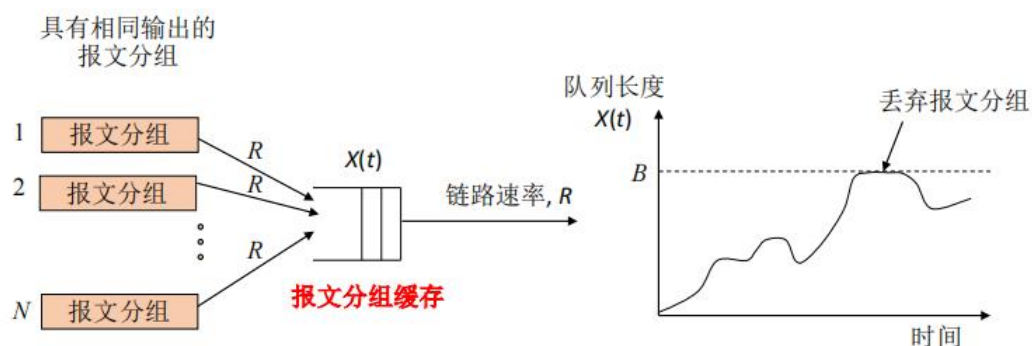
主机 A 和 B 的报文分组没有固定的到达模式，带宽按需共享，这种方式称为统计多路复用（statistical multiplexing）

报文交换为发送一个信息整体，如一个文件。

分组交换是将报文拆分成相对较小的数据包，会产生额外的开销，并且需要报文的拆分和重组。

分组交换实际上使用的是统计多路复用。

报文交换与分组交换均采用存储-转发交换方式。



解答：

1、时延的不确定性：

- 在路由器中的处理时间：需要进行差错检验，确定输出链路等操作。
- 排队延迟：报文交换和分组交换采用的都是存储-转发的交换方式，若在同一

时间内，到达了很多的分组，他们需要进行排队，由于转发速率和缓冲区大小的限制，可能会出现**丢包或拥塞**的情况，此时就需要进行重传或等待，丢包情况会增加时延。

- 分组大小和分组数量，数据流的个数，数据流占带宽的频率，都会影响时延。

2、在单一链路中， $\text{latency} = \text{prop} + \text{transp}$ ，而 $\text{prop} = L/C$ ， $\text{transp} = P/R$ ，显然，对于端到端的传输，不管是单链路还是统计多路复用，其时延与**电磁波传播速度 C**，**链路长度 L**，**报文长度 P**，**传输速率 R** 有关。

- 电磁波传播速度 C：在不同介质中电磁波的传播速度不一样，该影响因素的根本原因是传输介质。

- 链路长度 L：长度越长，时延越长，反之亦然。
- 报文 P 越长，时延越长
- 传输速率 R 越大，时间越短

第二章问题：

Q1: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。

解答：

结果截图：



```
D:\homework\network\书面作业一>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: 220.181.38.150
           220.181.38.149
Aliases:  www.baidu.com
```

服务器: Unknown

在命令行输入 nslookup www.baidu.com 后，出现了服务器: unknown 的情况。这里其实给出的是 **DNS 服务器域名**

原因：这是由于搭建内部 DNS 服务器时我们一般习惯性只使用默认的正常查找区域，也就是只使用 DNS 服务器把域名解析成 IP 地址的功能。实际上 DNS 服务器还有一个反向查找区域，就是能把 IP 地址解析成域名。出现上述情况，是因为没有创建反向查找区域，DNS 服务器无法根据自己的 IP 地址解析成对应的域名。

解决方法：

使用 DNS 管理器，创建反向查找区域，并在正常查找区域的主机 A 记录属性中添加指针。

一般每个 ISP(互联网服务提供商)都部署有域名服务器，其用户可将该服务器设置成本地域名服务器（或默认域名服务器），如果我们想要得到一个有名字的本地 dns 域名服务器，可以先使用 nslookup，再使用 server 8.8.8.8 将谷歌的开放 dns 服务器设置为本地域名服务器，并在这期间使用 wireshark 捕获交互过程。

```
D:\homework\network\书面作业一>nslookup
默认服务器: UnKnown
Address: 222.30.45.41

> server 8.8.8.8
默认服务器: dns.google
Address: 8.8.8.8

> www.baidu.com
服务器: dns.google
Address: 8.8.8.8

非权威应答:
名称: www.a.shifen.com
Addresses: 14.215.177.38
          14.215.177.39
Aliases: www.baidu.com
```

设置本地域名服务器

服务器: dns.google

Address: 8.8.8.8

这一部分是本地 dns 域名服务器的信息，包含了域名和 ip，可以使用默认的（也就是默认域名服务器），也可以使用指定的（如本实验中将 google 部署的域名服务器设置为本地域名服务器。）

非权威应答:

权威 DNS 服务器，在自己的配置文件中直接写明了域名与主机对应关系并被授权管理该域时，可以认为这个 dns 是该域的权威 dns。（查阅资料）

本次实验中，本地 dns 域名服务器没有域名 www.baidu.com 对应的 ip 信息，所以当有客户端通过本地 dns 域名服务器请求域名 www.baidu.com 时，不能立刻返回，而是需要通过反复解析或递归解析的方式在其他 dns 域名服务器上获得域名对应 ip。同时，请求的域名和 ip 对应关系也会在本地图名服务器上进行缓存。

所以我们在缓存中找到的对应关系而不是配置文件中写明的对应关系，故该 dns 服务器查询的域就不是权威 dns。

名称: www.a.shifen.com

Addresses: 220.181.38.149

220.181.38.150

Aliases: www.baidu.com

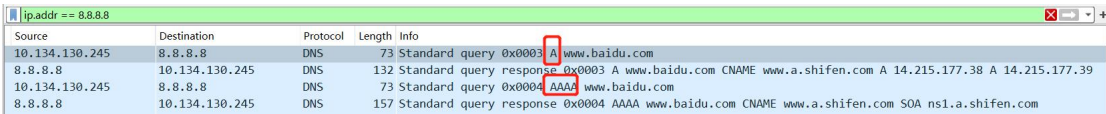
查询的域名为 www.baidu.com，得到的域名为 www.a.shifen.com（以前百度

叫十分网，后弃用），和别名(aliases)www.baidu.com，说明一个网站可能会有多个域名。

一个域名理论上可以对应多个 IP，而在用户访问过程中，指向某一个具体 IP，并不会同时访问多个 IP。但不同用户在不同地点访问同一个域名，可能会访问到不同的 IP 地址，但表象仍旧是这个域名。服务器将根据各地的访问 IP，到达域名 IP 中路由跳数最小的那个 IP 地址作为访问的域名 IP 地址。这样能保证一个域名被访问时，高速且稳定。

Wireshark 捕获过程:

(1)整体过程



| Source | Destination | Protocol | Length | Info |
|----------------|----------------|----------|--------|---|
| 10.134.130.245 | 8.8.8.8 | DNS | 73 | Standard query 0x0003 A www.baidu.com |
| 8.8.8.8 | 10.134.130.245 | DNS | 132 | Standard query response 0x0003 A www.baidu.com CNAME www.a.shifen.com A 14.215.177.38 A 14.215.177.39 |
| 10.134.130.245 | 8.8.8.8 | DNS | 73 | Standard query 0x0004 AAAA www.baidu.com |
| 8.8.8.8 | 10.134.130.245 | DNS | 157 | Standard query response 0x0004 AAAA www.baidu.com CNAME www.a.shifen.com SOA ns1.a.shifen.com |

本机 ip: 10.134.130.245

域名服务器 ip: 8.8.8.8

在我们的实验中，本机向域名服务器提交了两个解析域名的请求，通过课上的知识，我们知道。

A: 将名称对应到 IPv4 的 32 位地址

AAAA: 将名称对应到 IPv6 的 128 位地址

故第一次请求解析 ipv4 地址，第二次请求解析 ipv6 地址。

每次请求后域名服务器对本机进行应答 response

(2)以请求解析 ipv4 地址为例

Dns 报文格式如图所示：

■ DNS包括query和reply两种报文

| | | |
|--------------------------------|----|----------------------|
| 0 | 16 | 31 |
| IDENTIFICATION | | PARAMETER |
| NUMBER OF QUESTIONS | | NUMBER OF ANSWERS |
| NUMBER OF AUTHORITY | | NUMBER OF ADDITIONAL |
| QUESTION SECTION | | |
| ... | | |
| ANSWER SECTION | | |
| ... | | |
| AUTHORITY SECTION | | |
| ... | | |
| ADDITIONAL INFORMATION SECTION | | |
| ... | | |

• 请求报文

第一条捕获的数据为本机向 dns 域名服务器发送解析域名 www.baidu.com 的 ipv4 地址的请求，打开该捕获数据，其结果与 dns 报文存在一一对应关系

```

v Domain Name System (query)
  Transaction ID: 0x0003
  v 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: 350]

```

DNS 的请求报文头部:

Transaction Id 是事务的 ID(对应 IDENTIFICATION)

Flags 是报文中的标志字段(对应 PARAMETER), Response 字段为 0 是因为这个包是一个请求包, OPCODE 为零代表着标准查询, Truncated 是 TC 字符, Recursion desired RD 期望递归, 该字段能在一个查询中设置, 并在响应中返回。该标志告诉名称服务器必须处理这个查询, 这种方式被称为一个递归查询。reserved 保留位为 0, Questions 问题计数为 1, 其余的回答资源记录数、权威名称服务器计数以及附加资源记录数均为 0。

在报文格式中都能找到一一对应关系。

• 响应报文

```

v Domain Name System (response)
  Transaction ID: 0x0003
  v 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 authenticated by the server
    .... .... ..0 .... = Non-authenticated data: Unacceptable
    .... .... ..0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0

```

DNS 的响应报文头部:

响应事务 ID 与对应请求报文的事务 ID 相对应, 报文中的标志字段为回应, 并且应答没有错误, 使用递归查询, 其余参数为 0, Questions 问题计数为 1, 其余的回答资源记录数计数为 3, 权威名称服务器计数、附加资源记录数均为 0。

• 返回的具体内容

```

  ▾ Queries
    ▾ www.baidu.com: type A, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
    ▾ 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: 810 (13 minutes, 30 seconds)
        Data length: 15
        CNAME: www.a.shifen.com
      ▾ www.a.shifen.com: type A, class IN, addr 14.215.177.38
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 172 (2 minutes, 52 seconds)
        Data length: 4
        Address: 14.215.177.38
      ▾ www.a.shifen.com: type A, class IN, addr 14.215.177.39
        Name: www.a.shifen.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 172 (2 minutes, 52 seconds)
        Data length: 4
        Address: 14.215.177.39
\[Request In: 349\]
[Time: 0.057606000 seconds]

```

Name: 域名

Class: Class 是用来识别网络的信息，但目前除了互联网已经没有任何其他网络了，因此，Class 只有一个 IN 值；

type 类型: 表示该域名映射对应的类型，当类型为 A，表示 DNS 服务器上域名映射的是 Ipv4 地址；当类是 CNAME 时，表示是一个别名；

Time To Live: DNS 使用区域数据库存储名字与地址映射关系，映射关系的有效时间

Data Length: 代表了数据的长度

Cname: 别名

Address: 地址

• ipv6 响应报文的区别


```

  v Queries
    v www.baidu.com: type AAAA, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
  v Answers
    v 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: 796 (13 minutes, 16 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
  v Authoritative nameservers
    v a.shifen.com: type SOA, class IN, mname ns1.a.shifen.com
      Name: a.shifen.com
      Type: SOA (Start Of a zone of Authority) (6)
      Class: IN (0x0001)
      Time to live: 216 (3 minutes, 36 seconds)
      Data length: 45
      Primary name server: ns1.a.shifen.com
      Responsible authority's mailbox: baidu_dns_master.baidu.com
      Serial Number: 2211210024
      Refresh Interval: 5 (5 seconds)
      Retry Interval: 5 (5 seconds)
      Expire limit: 2592000 (30 days)
      Minimum TTL: 3600 (1 hour)
\[Request In: 351\]
[Time: 0.057054000 seconds]

```

查阅资料，我们可以知道，DNS 名称服务器保存着域名空间中部分区域的数据。如果 DNS 服务器负责管辖一个或多个区域时，称此 DNS 服务器为这些区域的**授权服务器（Authoritative NameServer）**。

名称服务器（Name Server）资源记录用于标记被指定为区域权威服务器的 DNS 服务器。通过在 NS 资源记录中列出服务器，其他服务器就认为它是该区域的权威服务器。这意味着在 NS 资源记录中指定的任何服务器都被其他服务器当作权威的来源，并且能肯定应答区域内所含名称的查询。

在请求分析 ipv6 地址的 dns 响应报文中，相比 ipv4，增加了授权服务器以及描述响应信息相应的参数。

Q2:

(1) 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）。

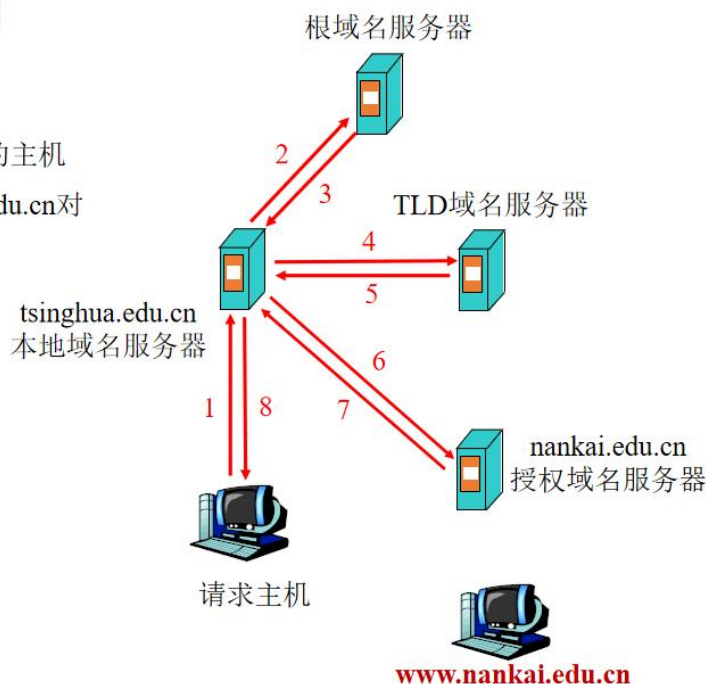
DNS域名解析示例

■ 例如：

- ▶ tsinghua.edu.cn域中的主机
要解析www.nankai.edu.cn对应的IP地址

■ 解析过程

- ▶ 反复解析
- ▶ 递归解析



反复解析的过程

- 首先，在本机缓存(浏览器，应用和操作系统等)中查找域名和 ip 的对应关系，若有缓存则直接返回对应 ip。
- 若本机缓存中没有对应关系，则向本地 DNS 域名服务器发送解析请求，在本地域名服务器的缓存中查找域名和 ip 的对应关系，若有缓存则直接返回域名对应的 ip。
- 若本机缓存和本地域名服务器缓存中都没有地址和 ip 的对应关系，则将解析请求发给根域名服务器，根服务器知道所有顶级域名服务器的 ip 地址，向本地域名服务器返回可解析该域名的 TLD(顶级域名服务器)ip
- 本地 DNS 服务器根据上一步获得的顶级 DNS 服务器 ip 向其发送域名解析请求，TLD 域名服务器返回一个可解析该域名的授权域名服务器的 ip
- 本地 DNS 服务器根据上一步获得的授权域名服务器 ip 向该 ip 发送解析请求，授权域名服务器是保存着名字与地址映射，保留其初始数据来源的服务器，用来保存所有其所管辖的主机域名到 ip 地址的映射，授权域名服务器对域名进行解析，并将结果返回给本地域名服务器。
- 本地域名服务器将解析结果返回给本机。

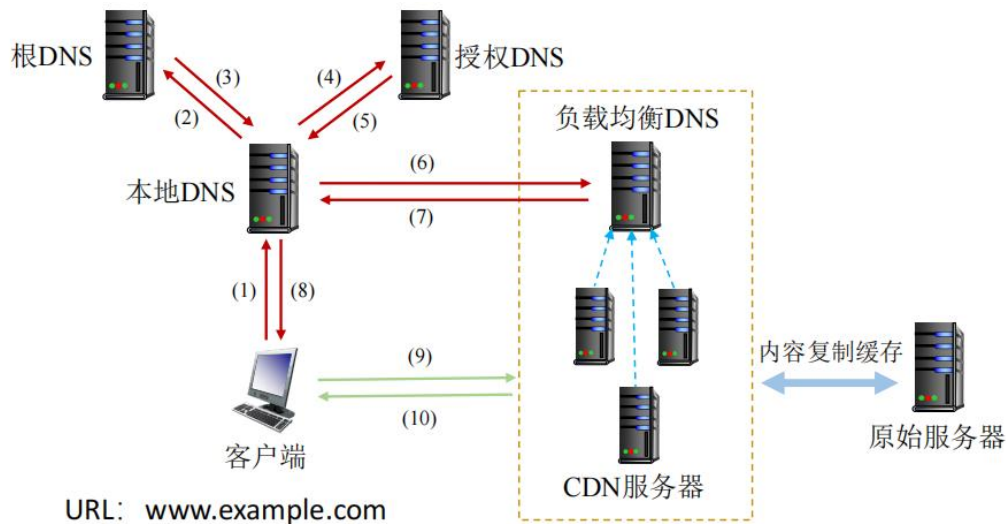
在这里，我认为我们要了解授权服务器的概念！

DNS 名称服务器保存着域名空间中部分区域的数据。如果 DNS 服务器负责管辖一个或多个区域时，称此 DNS 服务器为这些区域的**授权服务器 (Authoritative NameServer)**。

名称服务器 (Name Server) 资源记录用于标记被指定为区域权威服务器的 DNS 服务器。通过在 NS 资源记录中列出服务器，其他服务器就认为它是该区域的权威服务器。这意味着在 NS 资源记录中指定的任何服务器都被其他服务器当作权威的来源，并且能肯定应答区域内所含名称的查询。

即，若解析请求来到了授权服务器，若域名有效，则一定能解析，若解析不了，则说明要求解析的域名不存在对应的 ip。

(2) 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。



CDN 中的 DNS 重定向的基本方法和过程：

在内容分发网络中，客户端的域名解析请求首先发送给本地 DNS，若本地 DNS 有缓存则直接返回，若没有，则将解析请求发送给根 DNS，根 DNS 根据域名返回本地 DNS 一个授权 DNS 的 ip，本地 DNS 继续将解析请求发送给负载均衡的 DNS。（查阅资料，事实上负载均衡 DNS 是个笼统的概念，先访问全局负载均衡 DNS，再访问区域负载均衡 DNS）。

负载均衡 DNS 使用调度算法，根据客户端的 ip 地址和 CDN 系统每台机器的负载情况，找到一个合适的 CDN 服务器，并将其 ip 地址返回给客户端。

客户端通过返回的 ip 直接于 CDN 服务器进行交互。

若交互的 CDN 服务器缓存中有请求内容，则直接返回，若没有，则在 CDN 网络集群中逐级向上层服务器请求，若上层服务器缓存中有请求的内容，则逐级缓存并返回。（若缓存中都没有，则请求最终到达原始服务器，并逐级缓存并返回）

原始资源记录的修改：

需要重写授权 DNS 的资源记录，将请求域名的 A 类型记录改为 Cname 记录，添加请求域名和 Cname 的对应关系。

如：

原始资源记录为：

www.baidu.com A 百度真实 ip

修改为资源记录（实现的方式可以有多种，这里仅展示一种，目标就是返回负载均衡 DNS 域名的真实 ip）

www.baidu.com Cname 负载均衡 DNS 域名

负载均衡 DNS 域名 NS 负载均衡 DNS 域名真实 ip

经过这样的修改，在向授权服务器请求域名解析时，授权服务器才能返回给本地 DNS 域名服务器负载均衡 DNS 的真实 ip

Q3: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 包括 *query* 和 *reply* 两种报文

| | | |
|---------------------------------------|----|----------------------|
| 0 | 16 | 31 |
| IDENTIFICATION | | PARAMETER |
| NUMBER OF QUESTIONS | | NUMBER OF ANSWERS |
| NUMBER OF AUTHORITY | | NUMBER OF ADDITIONAL |
| QUESTION SECTION ... | | |
| ANSWER SECTION ... | | |
| AUTHORITY SECTION ... | | |
| ADDITIONAL INFORMATION SECTION ... | | |

解答：

UDP 提供的是不可靠的传输服务，解析域名时需要应用层的来保障。

报文中的 PARAMETER，暂且理解其为参数，对应 wireshark 捕获的交互过程中报文头部的 flags，flags 中的最后四位为 0000，并给出 Reply code: No error(0)，在 flags 所在行也给出了 No error 的提示，说明没有错误。

DNS 数据包中，可以比较问题的数量和回答的数量，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 地址的数目也是检验的依据。将发送报文和响应报文的事务 ID 需要匹配，可以进行一定程度的检验。

在响应报文中，answers 中有对应响应的 Time to live，TTL 表示资源记录的生命周期，使用 TTL 定期对更新缓存资源，保证数据的正确性。

UDP 不是面向连接的通信，发送消息前不会进行连接确认，若 DNS 服务器发生宕机，大量域名将无法被解析，因此，DNS 协议通过部署多台冗余服务器避免单点消失。冗余服务器(又称辅 DNS 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。