### 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\*108米/秒）

知识点：



链路1：

传输速率R1=100Mbps=1x108bit/s

链路长度L1=4000m

链路2：

传输速率R2=10Mbps=1x107bit/s

链路长度L2=2000m

报文长度=P10000字节=80000bit

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

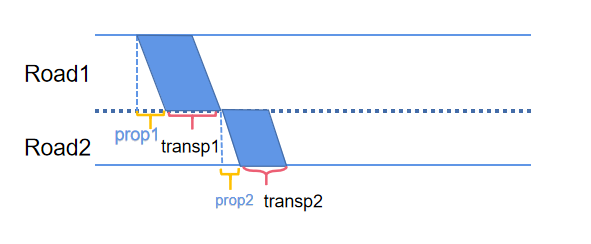
prop1：链路1上的传播时延

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



prop1==4000m/(2\*108)m/s=2x10-5=0.02x10-3s

transp1==80000bit/108bit/s=8x10-4=0.8x10-3s

prop2==2000m/(2\*108)m/s=1x10-5=0.01x10-3s

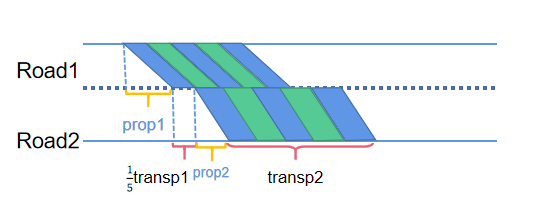
transp2==80000bit/107bit/s=8x10-3s

**latency=prop1+transp1+prop2+transp2=(0.02+0.8+0.01+8)x10-3s=8.83x10-3s**

**= 8.83(ms)**

1. 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）。

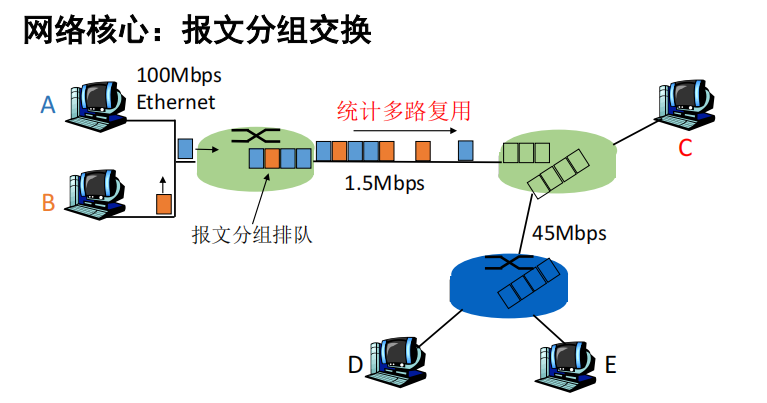
解答：在第一问中，我们知道了transp1<transp1，所以不会出现第一个分组在Road2上传输完毕但第二个分组还在Road1上传输的情况，即Road2上的第k(0<=k<=4)个分组传输完毕后立刻传输下一个分组。



**latency=prop1+transp1+prop2+transp2=(0.02+0.16+0.01+8)x10-3s=8.18x10-3s**

**= 8.19(ms)**

1. 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：****

**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

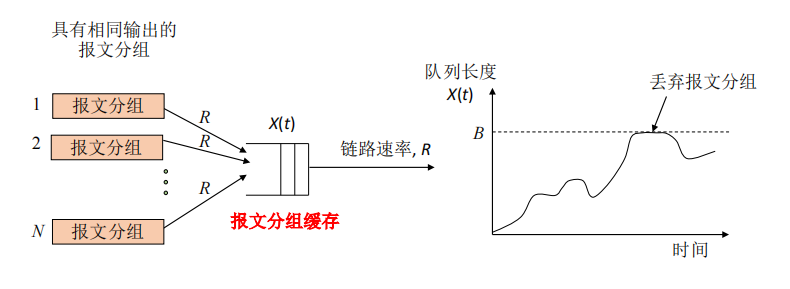
种方式称为**统计多路复用**（statistical multiplexing）

**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。

1. 在单一链路中，latency=prop+transp，而prop=L/C，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：**



**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。



**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域名服务器上进行缓存。

所以我们是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**

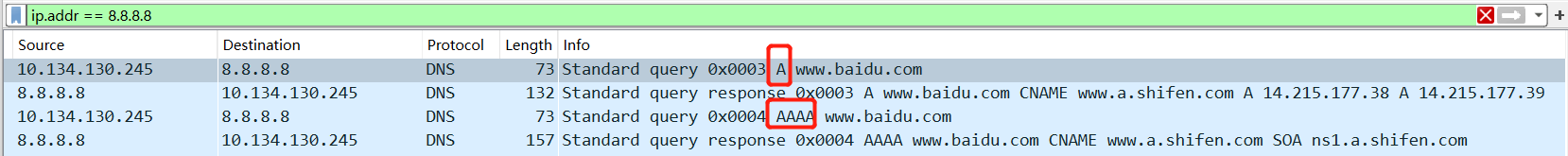
**Aliases: www.baidu.com**

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**



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

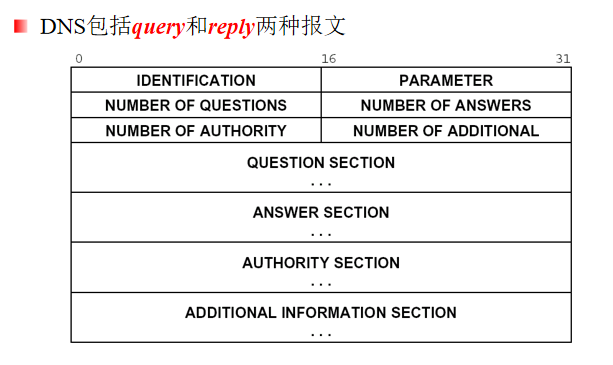
AAAA： 将名称对应到IPv6的128位地址

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

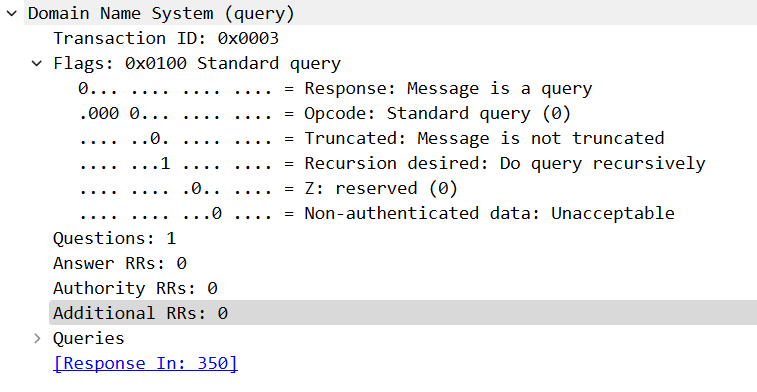
**(2)以请求解析ipv4地址为例**

Dns报文格式如图所示：



**· 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



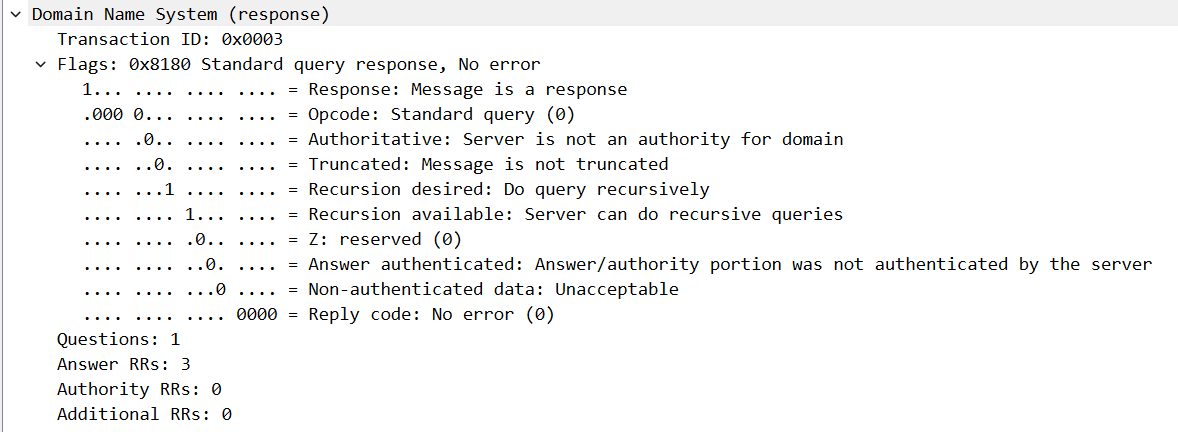
DNS的请求报文头部：

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，OPCOODE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。

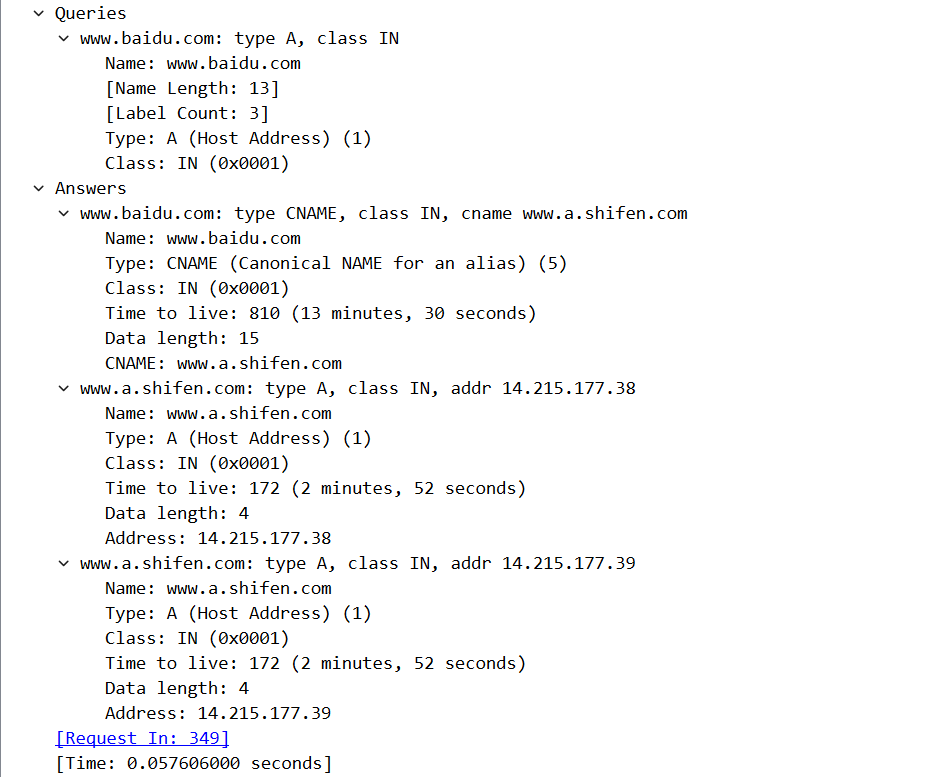
**·响应报文**



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**



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；

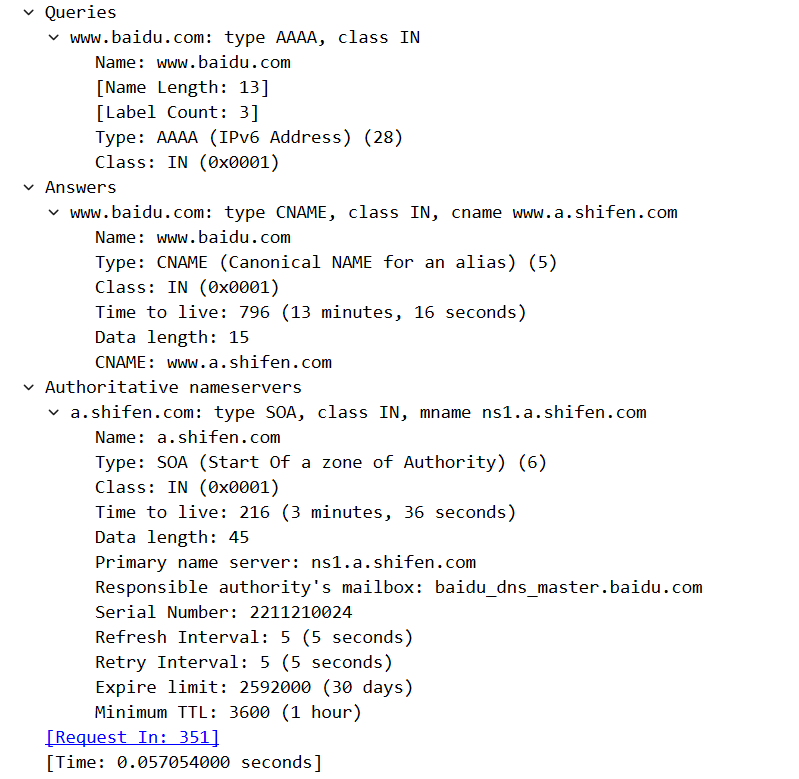
Time To Live：DNS使用区域数据库存储名字与地址映射关系，映射关系的有效时间

Data Length：代表了数据的长度

Cname：别名

Address：地址

**·ipv6响应报文的区别**



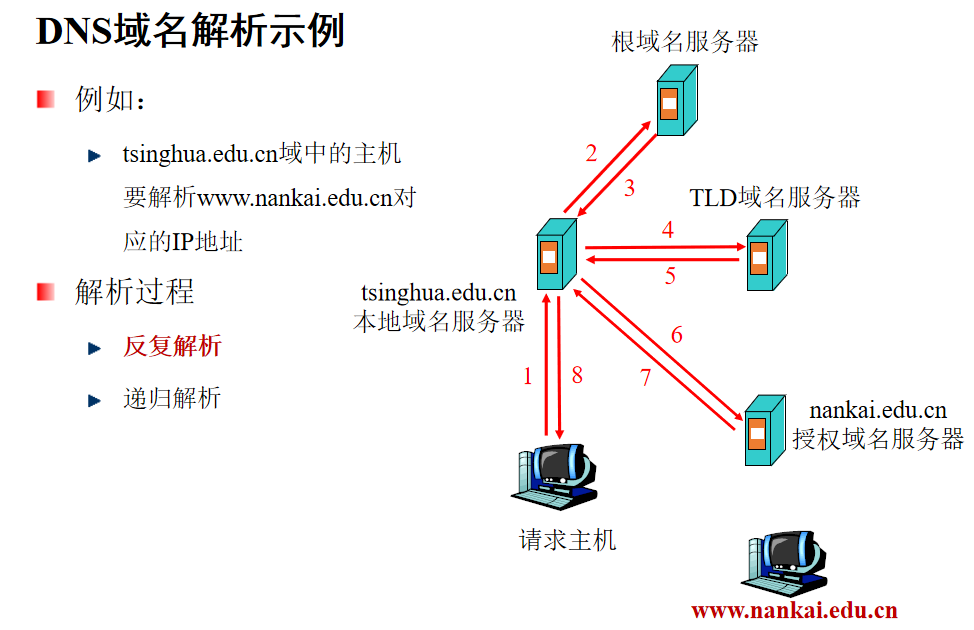
查阅资料，我们可以知道，DNS名称服务器保存着域名空间中部分区域的数据。如果DNS服务器负责管辖一个或多个区域时，称此DNS服务器为这些区域的**授权服务器（Authoritative NameServer）**。

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）。



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。

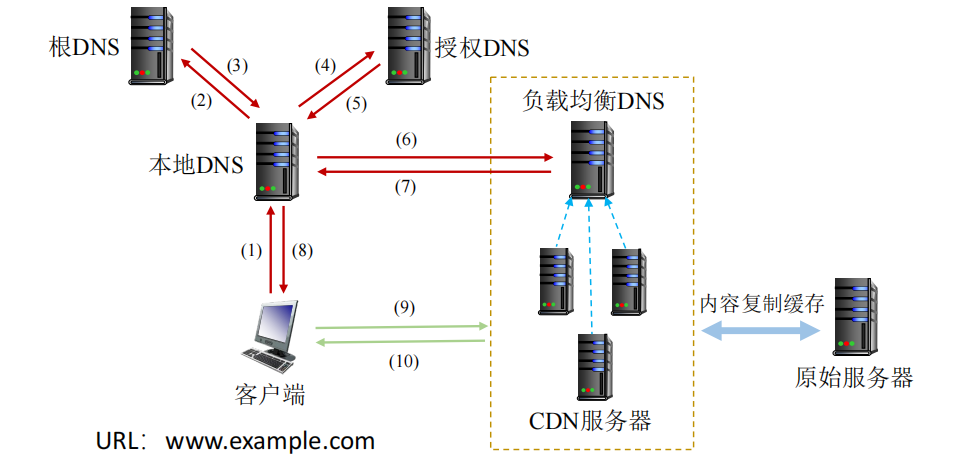
在这里，我认为我们要了解授权服务器的概念！

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**。

1. 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，再访问区域负载均匀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](http://www.baidu.com) A 百度真实ip

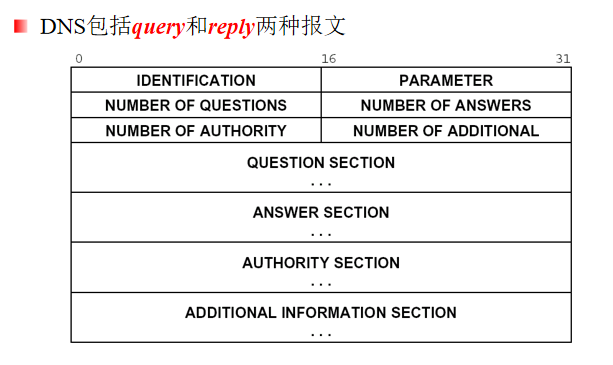
修改为资源记录（实现的方式可以有多种，这里仅展示一种，目标就是返回负载均衡DNS域名的真实ip）

[www.baidu.com](http://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。



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。