第一章作业

（1）

PROP = $\frac{4000}{2\times10^8}+\frac{2000}{2\times10^8}=\frac{6000}{2\times10^8}=3\times10^{-5}$（$s$）

TRANSP = $\frac{10000\times8}{100\times10^6}+\frac{10000\times8}{10\times10^6}=8\times10^{-4}+8\times10^{-3}=8.8\times10^{-3}$（$s$）

Latency=TRANSP+PROP=8.83×10^{-3}（s）

（2）

PROP = $\frac{4000}{2\times10^8}+\frac{2000}{2\times10^8}=\frac{6000}{2\times10^8}=3\times10^{-5}$（$s$）

TRANSP = $\frac{2000\times8}{100\times10^6}+\frac{10000\times8}{10\times10^6}=1.6\times10^{-4}+8\times10^{-3}=8.16\times10^{-3}$（$s$）

Latency=TRANSP+PROP=8.19×10^{-3}（s）

（3）

统计多路复用的核心思想是不需要将带宽提升至每一个数据流的峰值之和那么多，因为在真实的网络中流的峰值的出现具有突发性，是不平稳的，每个流的峰值可能出现在不同的时间，所以说可以将带宽设置在多个流的峰值之和以下以实现统计多路复用增益。

但是，如果网络中的数据流突然大规模出现，或者网络中多个流在一个时间段内都同时出现峰值，这就会导致统计多路复用后的带宽大小无法满足其共同传输的要求，可能会出现丢弃报文分组的情况出现。

所以说引入统计多路复用后，因为网络中流量的突发性以及不平稳，当数据量大规模同时出现时也会出现端到端延迟情况的出现，主要原因是数据在传输过程中可能被丢弃。

以上是由于统计多路复用机制的特点可能产生的延迟状况的原因，而在其他方面：传输速率、链路长度以及网络带宽都会影响端到端的时延，传输速率越大、链路长度越短、网络带宽越大则时延越小。并且如题目所示，如果在一个路由器的两段链路传输速率差异过大同样也会造成端到端的时延问题，因为传输速度大的链路被迫等待传输速率慢的链路导致整体传输速率变慢。

第二章作业

第一题：

查询域名的 IP 地址时出现了 DNS 服务器为 Unknown 的情况，查询了一下网上的资料是说没有配置域名的反向解析，我尝试了一下不太会，而且我觉得他返回的 Address 也不太对于是采用了一个新的办法。

于是我换了一个方法：将域名服务器切换到谷歌的开放 dns 服务器上，输入命令"server 8.8.8.8"，再做域名的解析就可以得到我们需要的答案了

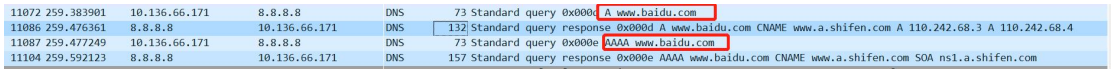
第一部分是本机使用的 DNS 服务器的信息，客户端先到主 DNS Server 进行连接查询

第二部分内容给我们返回了“非权威应答”。非权威应答的意思是假设某个 DNS 服务器没有域名 www.baidu.com 的信息，当有客户端通过它请求百度的 ip 地址时会通过反复解析或者递归解析的方式从欧诺个实际存储域名-ip 对应关系的 DNS 服务器中获取 baidu 的域名信息，获得后再反馈给客户端，同时，该域名服务器也会将记录信息放在缓存中，如果再其失效前再有客户端访问就可以直接返回给客户端。

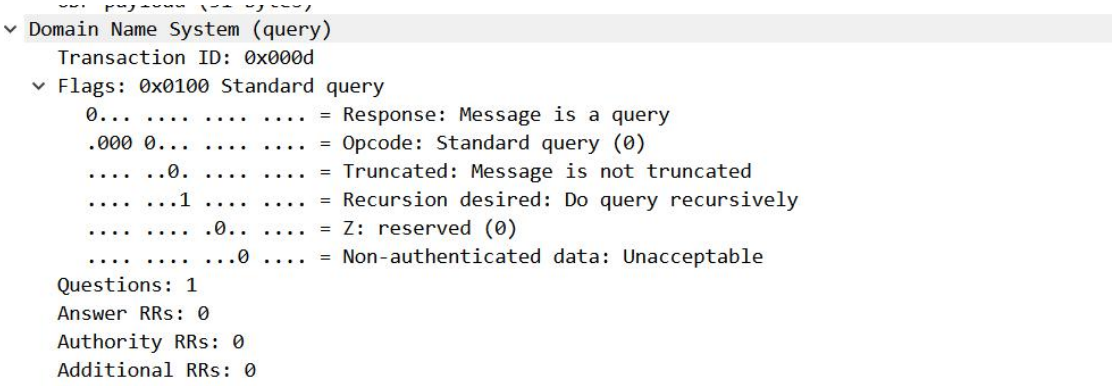
第三部分内容我们可以首先看到了一个 www.a.shifen.com，这说明一个网站很多时候都不止有一个域名，可能会拥有很多备用域名。上网查找了一下资料：www.a.shifen.com 是百度原来的域名,百度原来就叫十分网,因为点击量每点一下赚 10 分钱,现在作废了。然后可以看到 nslookup 返回了两个 ip 地址，也就是一个域名可能会对应多个 ip 地址，但是在用户对某一域名发起访问时只会对应到一个 ip 地址，但是在不同时间不同地点访问同一个域名可能会反馈回不同的 ip 地址。服务器会根据路由器中跳数最小的 IP 地址作为用户一次访问时的 IP 地址，这样做不仅可以保证提升访问效率，也可以通过多个 ip 地址映射提升系统的鲁棒性。最后一个 Aliases 顾名思义，就是别名的意思，是目标域名的别名。

然后我们来使用 wireshark 来捕获本次的查询结果，可以看到主机向 google DNS 提交了两次域名解析的请求，第一次是 A www.baidu.com，第二次是 AAAA www.baidu.com,两次的区别

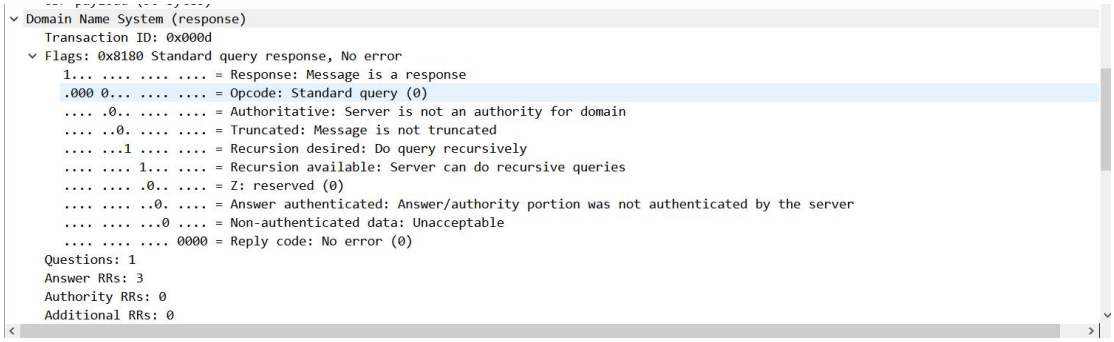
在于 A 是解析 IPV4 地址，第二次是请求解析 IPV6 地址



DNS 的请求包头部：TransactionId 是事务的 ID，Flags 是报文中的标志字段，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 字符安，Recursion 是 RD 字段，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



DNS 的响应包头部：事务 ID 与发出时的事务 ID 相对应，报文中的标志字段为返回，并且没有错误，QR 字段为 1 表示一个响应包，AA 字段、TC 字段、为 0，RD 和 RA 字段均为 1，并对一个问题返回了 3 个回答。



然后我们以 IPV4 的地址解析为例分析 google DNS 返回的内容：

首先，第一条回答的别名为 CNAME，表示这一个键值对返回的是域名的别名，也就是我们在命令行窗口处看到的名称 www.a.shifen.com

接下来两条得到的类型都为 A，也就是解析了 32 位的 IPV4 地址，分别解析出来了这个域名所对应的两个 ip 地址。

其他的一些参数例如 Time To Live 代表了有效时间，Data Length 代表了数据的长度，Class In 表示在新特网上搜索

```
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: 334 (5 minutes, 34 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
  www.a.shifen.com: type A, class IN, addr 110.242.68.3
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 110.242.68.3
  www.a.shifen.com: type A, class IN, addr 110.242.68.4
      Name: www.a.shifen.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 110.242.68.4
  [Request In: 11072]
  [Time: 0.092460000 seconds]
```

而在对 IPV6 的解析中看到了更加丰富的内容：在回答中出现了 Authoritative nameservers，我在网上也找到了关于授权服务器的定义，与理论课上学习的基本一致：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。

SOA 代表着区域数据库的开始，描述负责区域的域名服务器、版本信息以及从属域名服务器备份时的一些参数。

主要名称服务器：主要名称服务器（PrimaryNameServer），它保存着区域中的相关设置数据，当区域中的数据更改，如添加主机时，这些更改就被保存到主要名称服务器中。

Responsible authority’s mailbox 表示负责人（管理员）的邮箱等一些其他的信息，因为涉及到授权服务器，所以信息也比非授权的服务器要丰富些。

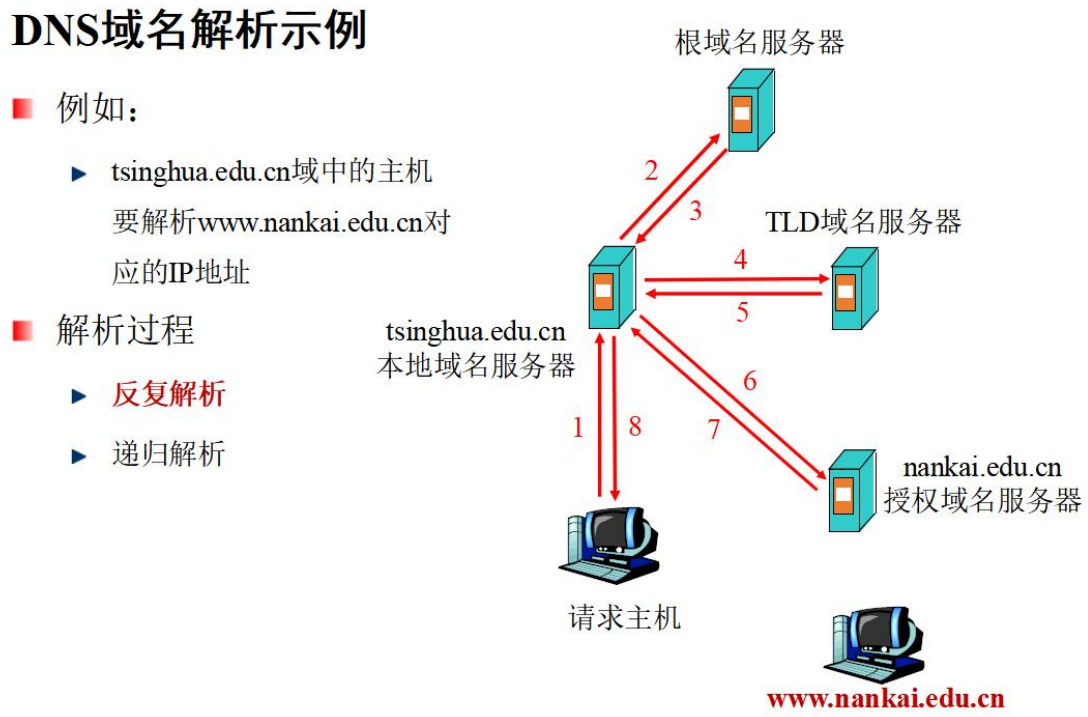
```
Queries
  www.baidu.com: type AAAA, class IN
      Name: www.baidu.com
      [Name Length: 13]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
Answers
  www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 1035 (17 minutes, 15 seconds)
      Data length: 15
      CNAME: www.a.shifen.com
Authoritative nameservers
  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: 600 (10 minutes)
      Data length: 45
      Primary name server: ns1.a.shifen.com
      Responsible authority's mailbox: baidu_dns_master.baidu.com
      Serial Number: 2211180030
      Refresh Interval: 5 (5 seconds)
      Retry Interval: 5 (5 seconds)
      Expire limit: 2592000 (30 days)
      Minimum TTL: 3600 (1 hour)
  [Request In: 11087]
  [Time: 0.114874000 seconds]
```

最后，由抓包结果可以分析，DNS 使用的是 53 端口，代表了其使用了 UDP 协议

```
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.136.31.112
v User Datagram Protocol, Src Port: 53, Dst Port: 63818
    Source Port: 53
    Destination Port: 63818
    Length: 98
```

第二题：

（一）以反复解析为例分析域名解析的基本过程



以 ppt 上的图为例说明 DNS 的解析过程。

首先，请求主机向本地域名服务器发起请求，本地域名服务器查看是否有该域名到 IP 地址的映射，如果有且未过期直接返回，如果没有就发给根域名服务器。

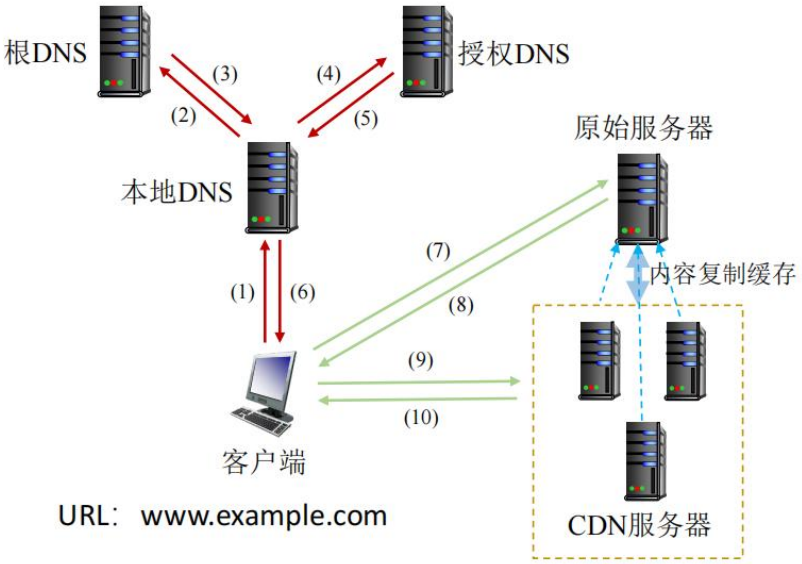
根局域名服务器是最高层级的域名服务器，根服务器知道所有顶级域名服务器的域名和 ip 地址，根域名服务器会向本地域名服务器发送负责该域名解析的 TLD 域名服务器地址。如果根域名服务器存在域名到 ip 的映射且未过期则直接返回 ip 地址。

顶级域名服务器负责管理管理在该顶级域名服务器注册的所有二级域名，当收到本地域名服务器的请求时给出相应的回答，这个回答可能是一个授权域名服务器的地址，也可以因为有未过期的缓存而直接返回正确的域名对应的 ip 地址。

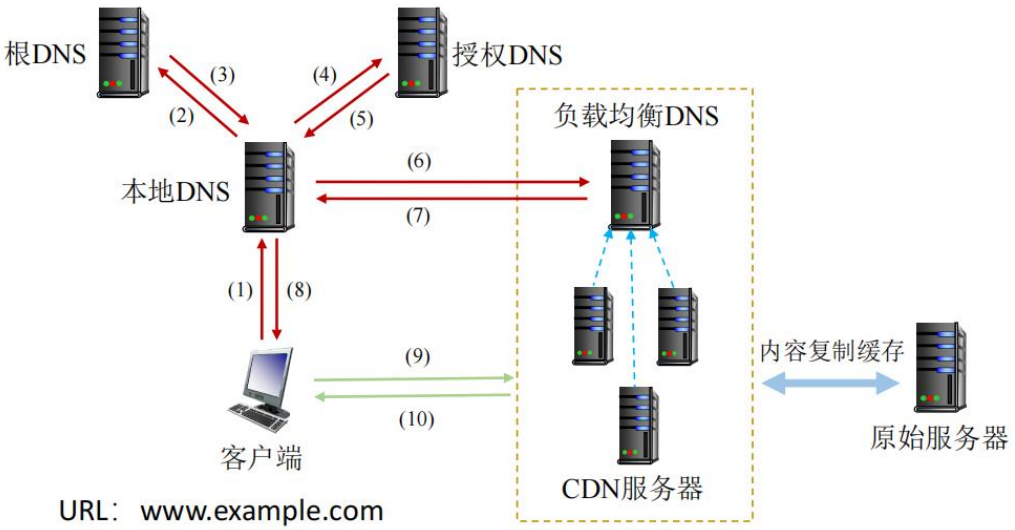
授权域名服务器是对于名字与地址映射，保留其初始数据来源的服务器，用来保存所有其所管辖的主机域名到 ip 地址的映射，授权域名服务器会将解析的结果返回给本地域名服务器，再由本地域名服务器传递给请求主机

（二）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

第一种内容分发网络的示意图如下图所示：客户端向本地 DNS 请求，本地 DNS 在经过和反复解析类似的步骤之后拿到了由授权 DNS 返回的原始服务器的 ip 地址，本地 DNS 将这个 IP 地址返回给客户端，客户端使用这个 ip 地址与原始服务器交互，但此时原始服务器并不会直接相应客户端的域名解析请求将域名解析，而是会返回一个 CDN 服务器的 ip 地址，在这些 CDN 服务器对原始服务器中的内容进行复制缓存，客户端通过与 CDN 服务器交互，由 CDN 服务器完成域名解析的工作。



第二种内容分发网络的特点是，客户端不会与原始服务器进行交互，如下图所示：



在该内容分发网络中，客户端的解析请求将首先被发送至本地 DNS，如果本地 DNS 无法根据缓存完成域名解析，本地 DNS 会将请求发送至根 DNS，并由 DNS 返回一个授权 DNS 的 IP 地址，并由该 IP 地址给出负载均衡 DNS 的 IP 地址。

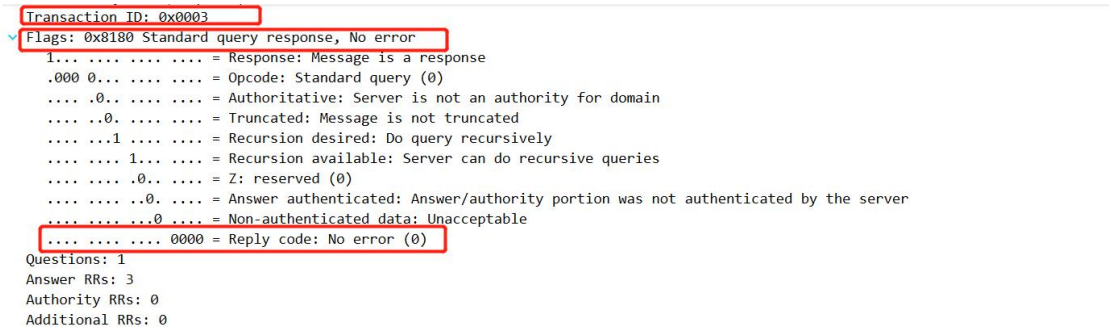
负载均衡 DNS 负责决策 CDN 服务器选择，负载均衡 DNS 需要收集 CDN 服务器的位置和负载情况，如果找不到被请求的对象，需要从原始服务器获取。负载均衡 DNS 会根据下属各个

CDN 服务器服务器的工作状况以及传输效率等因素综合考量，返回给本地 DNS 一个最合适的 CDN 服务器的 IP 地址，本地服务器会将该 IP 地址返回给客户端。

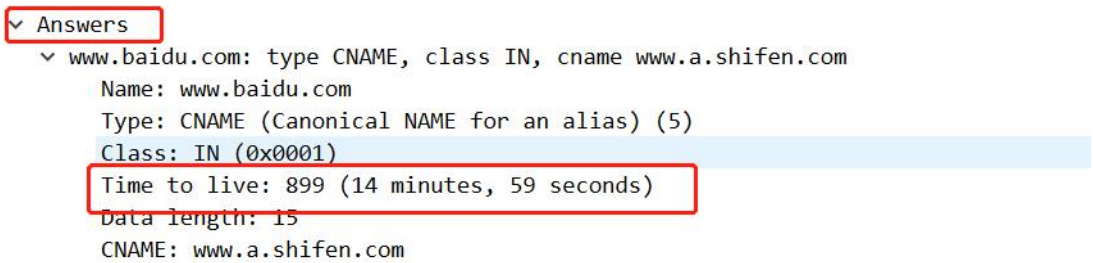
客户端将通过该 IP 地址定位到一个 CDN 服务器并根据该 CDN 服务器与原始服务器的交互进行域名解析或者根据缓存进行域名解析，最后返回的值完成对域名的解析。

第三题：
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 协议的可靠机制可以由应用层来保障。具体保障的手段可以参考 TCP 所使用的校验和验证（差错重传）以及超时重传。例如在应用层进行校验和的计算并且根据发送的域名解析请求进行计时，如果超时则再次重复进行域名解析请求。
除此之外还要充分利用 DNS 数据包的特殊结构来帮助我们完成检测，比如说：在之前的 wireshark 抓包中，我们可以看到两处被标明了 No error，分别在 Flags 位置以及 Reply Code 的位置，我们可以根据数据包头部的标志位以及 ReplyCode 来判断数据是否可能存在破损，例如，一个请求数据报的 OPCode 应该是 1，根据这样的检测也可以检测出数据报是否可能存在传输时的差错。



并且，每一个由 DNS 返回的解析结果并不是随时有效的，可以观察到在一次回答中同样包含一个 TimeToLive 的作用域：当超过了 TTL 规定的时间后，该回答就会自动失效，保证了每一次回答的有效性以及实时性。



并且，仔细观察其头部：

事务ID（Transaction ID）	标志（Flags）
问题计数（Questions）	回答资源记录数（Answer RRs）
权威名称服务器计数（Authority RRs）	附加资源记录数（Additional RRs）
查询问题区域（Queries）	
回答问题区域（Answers）	
权威名称服务器区域（Authoritative nameservers）	
附加信息区域（Additional records）	

DNS 数据报的头部记录了问题的计数、回答资源记录数等等，可能通过这些信息于世界查询问题区域的数量进行比较来判断是否可能存在差错或者丢包的发生。

最后，因为 UDP 不是面向连接的通信方式，所以在发送消息之前不需要进行连接确认，所以说如果 DNS 服务器损坏，将会造成大量域名无法解析的情况发生，于是 DNS 体系也在不同区域范围内部署多台冗余服务器来避免单点丢失，弥补 UDP 的劣势。