

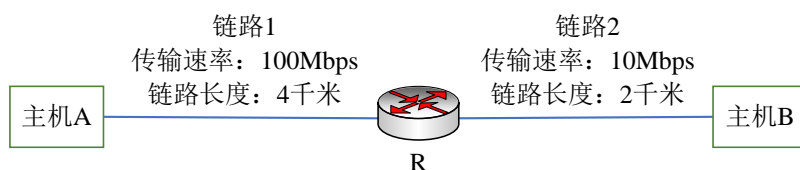
第一章问题

计算机科学与技术 2013536 汤清云

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. 报文大小: $10000 \times 8 = 80000 \text{ bit}$

(1) $PROP1 = \frac{L1}{C} = \frac{4000 \text{ m}}{2 \times 10^8 \text{ m/s}} = 2 \times 10^{-5} \text{ s}$
 $TRANSP1 = \frac{P}{R1} = \frac{80000 \text{ bit}}{1 \times 10^8 \text{ bit/s}} = 8 \times 10^{-4} \text{ s}$
 $PROP2 = \frac{L2}{C} = \frac{2000 \text{ m}}{2 \times 10^8 \text{ m/s}} = 1 \times 10^{-5} \text{ s}$
 $TRANSP2 = \frac{P}{R2} = \frac{80000 \text{ bit}}{1 \times 10^7 \text{ bit/s}} = 8 \times 10^{-3} \text{ s}$
 $Latency_{min} = PROP1 + PROP2 + TRANSP1 + TRANSP2 = 8.83 \times 10^{-3} \text{ s}$

(2) 传播时延无影响. $PROP = PROP1 + PROP2 = 3 \times 10^{-5} \text{ s}$
一个报文分组在链路1上的 $TRANSP1 = \frac{80000 \text{ bit}}{5 \times 10^8 \text{ bit/s}} = 1.6 \times 10^{-4} \text{ s}$
一个报文分组在链路2上的 $TRANSP2 = \frac{80000 \text{ bit}}{5 \times 10^7 \text{ bit/s}} = 1.6 \times 10^{-3} \text{ s} > TRANSP1$
 $TRANSP = TRANSP1 \times 5 + TRANSP2 \times 5 - TRANSP1 \times 4$
 $= TRANSP1 + 5 \times TRANSP2$
 $= 1.6 \times 10^{-4} \text{ s} + 8 \times 10^{-3} \text{ s}$
 $= 8.16 \times 10^{-3} \text{ s}$
 $Latency_{min} = TRANSP + PROP = 8.19 \times 10^{-3} \text{ s}$

示意图 A

影响端到端时延的主要因素:

1. 处理时延, 即检查分组首部, 决定分组导向需要的时间和检查比特级别的差错需要的时间。
2. 排队时延, 即分组在链路上等待传输的时间。取决于前期到达的正在排队等待向链路传输分组的数量。
3. 传输时延, 将所有分组的比特推向链路的时间。主要受链路传输速率的影响
4. 传播时延, 即比特上路后, 在起点到路由器之间传播需要的时间。

在统计多路复用中，主机之间没有固定的报文分组到达方式，带宽按需共享，由于数据通信的单个流稳定性差，因此统计多路复用能节省资源，但是会增加时延不稳定性，主要是由于网络中队列或者缓冲导致的抖动难以精准预测

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。

```
无线网络适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : 
    IPv6 地址 . . . . . : 2001:250:401:6566:d15a:caab:79aa:eea6
    临时 IPv6 地址. . . . . : 2001:250:401:6566:6911:9131:6923:6ff1
    本地链接 IPv6 地址. . . . . : fe80::a7a7:15cd:6c75:833%26
    IPv4 地址 . . . . . : 10.136.25.83
    子网掩码 . . . . . : 255.255.128.0
    默认网关. . . . . : fe80::865b:12ff:fe5e:3607%26
                        10.136.0.1

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 . . . . . : 

以太网适配器 vEthernet (WSL):

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址. . . . . : fe80::fe0d:blef:9d37:76de%65
    IPv4 地址 . . . . . : 192.168.208.1
    子网掩码 . . . . . : 255.255.240.0
    默认网关. . . . . : 

C:\Users\汤清云>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: 182.61.200.6
           182.61.200.7
Aliases:  www.baidu.com
```

相关解释：

- 服务器代表的是 DNS 服务器名称，这里为 unknown
- Address 表示的是 DNS 服务器地址，本机电脑的 DNS 服务器地址为 222.30.45.41；

非权威应答结果中：

- 名称表示的是百度原来的网址；
- Addresses 是百度的 IP 地址群，根据已学内容可得知这是一个 B 类的 IPv4 地址；
- Alias 代表了目标域名

Wireshark 捕捉结果：

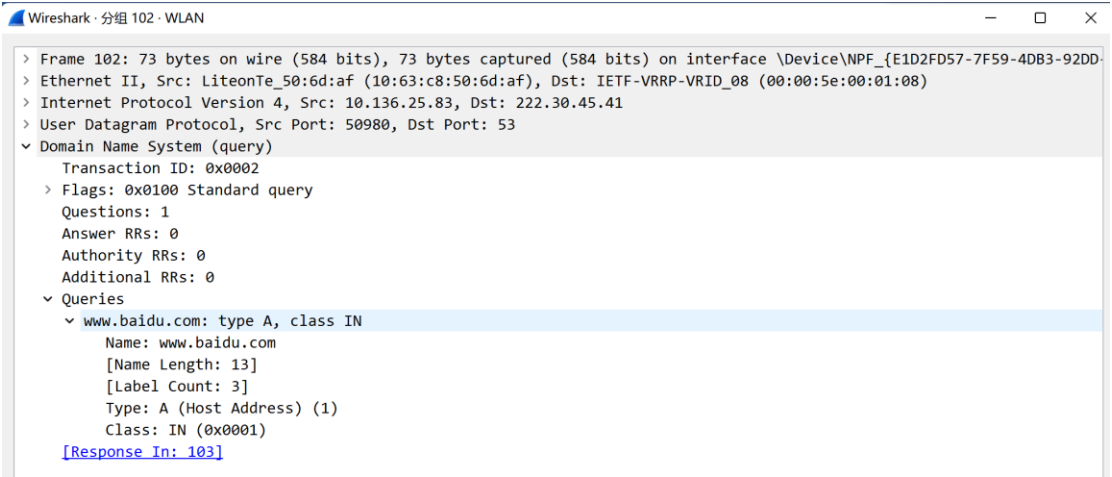
No.	Time	Protocol	Source	Destination	Length	Info
96	17.153363	TCP	10.136.25.83	103.212.12.52	54	51623 → 3000 [ACK] Seq=2 Ack=2 Win=512 Len=0
97	17.347946	ICMP	39.156.132.122	10.136.25.83	129	ICMP Protocol
98	17.786084	ICMPv6	fe80::865b:12ff:fe5e:ff02::1	ff02::1	118	Router Advertisement from 84:5b:12:5e:36:07
99	18.933094	TCP	10.136.25.83	20.205.243.166	54	52295 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
100	19.713888	TCP	218.28.198.190	10.136.25.83	60	[TCP Dup ACK 63#1] 443 → 54628 [ACK] Seq=1 Ack=1 Win=259 Len=0
101	19.713966	TCP	10.136.25.83	218.28.198.190	54	[TCP Dup ACK 64#1] 54628 → 443 [ACK] Seq=1 Ack=2 Win=513 Len=0
102	19.907806	DNS	10.136.25.83	222.30.45.41	73	Standard query 0x0002 A www.baidu.com
103	19.911916	DNS	222.30.45.41	10.136.25.83	132	Standard query response 0x0002 A www.baidu.com CNAME www.a.shifen.co...
104	19.916774	DNS	10.136.25.83	222.30.45.41	73	Standard query 0x0003 AAAA www.baidu.com
105	19.921249	DNS	222.30.45.41	10.136.25.83	157	Standard query response 0x0003 AAAA www.baidu.com CNAME www.a.shifen...
106	21.282826	TLSv1.2	10.136.25.83	140.143.219.189	81	Application Data
107	21.305635	TLSv1.2	140.143.219.189	10.136.25.83	81	Application Data
108	21.345682	TCP	10.136.25.83	140.143.219.189	54	52232 → 443 [ACK] Seq=136 Ack=136 Win=514 Len=0
109	21.776928	ICMPv6	fe80::865b:12ff:fe5e:ff02::1	ff02::1	118	Router Advertisement from 84:5b:12:5e:36:07
110	22.724151	TCP	2409:8c54:1050:10::...	2001:250:401:6566:6...	115	80 → 53463 [PSH, ACK] Seq=1 Ack=1 Win=3312 Len=41
111	22.727225	TCP	2001:250:401:6566:6...	2409:8c54:1050:10::...	447	53463 → 80 [PSH, ACK] Seq=1 Ack=42 Win=515 Len=373
112	22.787554	TCP	2409:8c54:1050:10::...	2001:250:401:6566:6...	74	80 → 53463 [ACK] Seq=42 Ack=374 Win=3321 Len=0

由以上捕捉结果可以看出：首先 nslookup 本机的地址是 10.136.25.83，即本地 WLAN 网络的 ipv4 地址，而服务器地址为 222.30.45.41，使用协议为 DNS。再对捕捉到的结果进行具体

分析如下：

- 下图（分组 102）为第一个包，其代表了首先本机向域名服务器发送查询请求，查询网址为 www.baidu.com，是一个 A 类的 ipv4 地址。同时可以由第四行看出 DNS 的查询报文是由 UDP 发送的。由于域名指向 ipv4 地址，因此第一个包增加了“A”记录标识。
- 第四行可以看出网络层为 ipv4 协议，源 ip 地址为 10.136.25.83；目的 ip 地址为 222.30.45.41
- 第五行表示传输层为 UDP 协议，源端口为 50980，目的端口为 53（DNS 默认使用端口）
- 应用层为 DNS 协议。

Transaction ID	标识字段，用来标识是哪个请求报文；
Flags	为 RD 置位，表示希望得到递归解答；
Questions	此处=1，表示请求数为 1；
Answer RRs	资源记录数，此处为 0；
Queries	为请求的域名，type A 表示为 ipv4 地址，地址类型为 class IN



```
Wireshark - 分组 102 - WLAN
> Frame 102: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{E1D2FD57-7F59-4DB3-92DD-...}
> Ethernet II, Src: LiteonTe_50:6d:af (10:63:c8:50:6d:af), Dst: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
> Internet Protocol Version 4, Src: 10.136.25.83, Dst: 222.30.45.41
> User Datagram Protocol, Src Port: 50980, Dst Port: 53
v Domain Name System (query)
  Transaction ID: 0x0002
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  v Queries
    v 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)
      [Response In: 103]
```

- 下图（分组 103）为第二个包，是服务器发回给本机的应答包，应答为 A 类域名，网址为 www.baidu.com，别名(CNAME)为 www.a.shife.com，IP 地址为 182.61.200.7 或 182.61.200.6。响应时间大约为 0.00411s

- 第四行可以看出网络层为 ipv4 协议，源 ip 地址为 10.136.25.83；目的 ip 地址为 222.30.45.41
- 第五行表示传输层为 UDP 协议，源端口为 50980，目的端口为 53（DNS 默认使用端口）
- 应用层为 DNS 协议

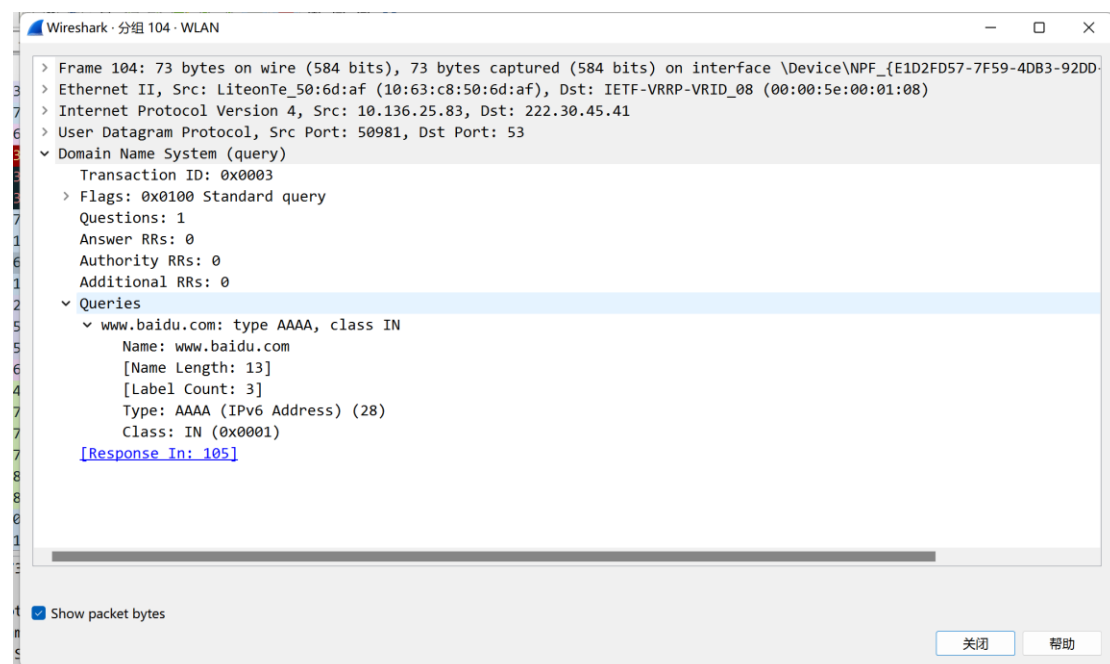
Transaction ID	用于辨别 DNS 应答报文是哪个请求报文的响应，值同请求报文；
Flags	此处 Response、RD、RA 置位，表示是应答报文，递归返回；
Questions	此处=1，表示请求数为 1；
Answer RRs	资源记录数，为 3，即有 3 条回复

具体应答如下图。

```
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
v Queries
  v 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)

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: 627 (10 minutes, 27 seconds)
    Data length: 15
    CNAME: www.a.shifen.com
  v 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: 286 (4 minutes, 46 seconds)
    Data length: 4
    Address: 182.61.200.7
  v 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: 286 (4 minutes, 46 seconds)
    Data length: 4
    Address: 182.61.200.6
[Request In: 102]
[Time: 0.004110000 seconds]
```

第三个包如下图，AAAA 代表此时主机名/域名指向了一个 IPV6 地址，其网址名为 www.baidu.com



第四个包如下，是对第三个包的应答包。SOA 叫做起始授权机构记录，NS 用于标识多台域名解析服务器，SOA 记录用于在众多 NS 记录中哪一台是主服务器。因此由下图可看出 a.shifen.com 为主服务器

```

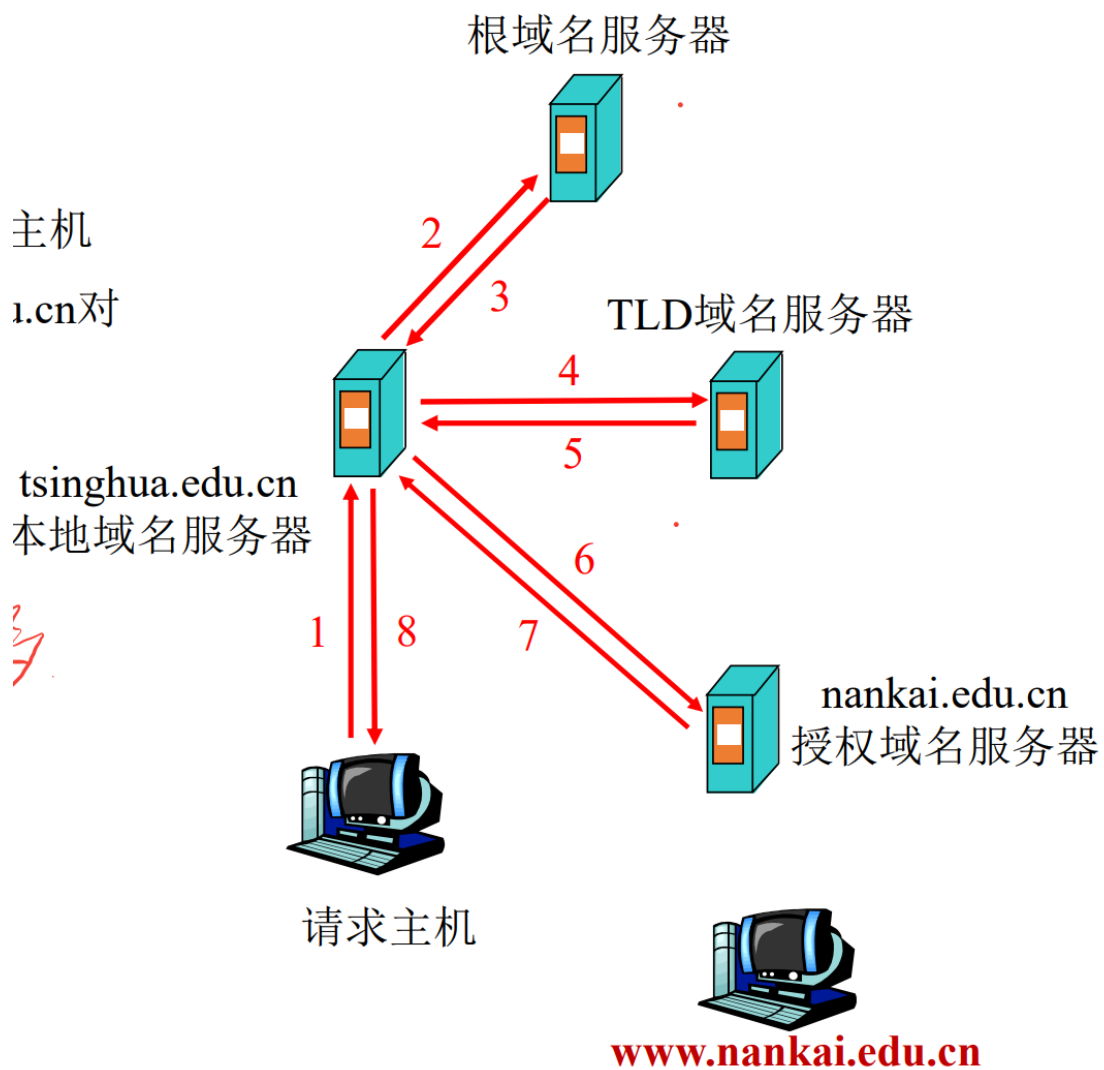
v Queries
  v www.baidu.com: type AAAA, class IN
    Name: www.baidu.com
    [Name Length: 13]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
  v Answers
    v www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
      Name: www.baidu.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 627 (10 minutes, 27 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: 12 (12 seconds)
      Data length: 45
      Primary name server: ns1.a.shifen.com
      Responsible authority's mailbox: baidu_dns_master.baidu.com
      Serial Number: 2211220037
      Refresh Interval: 5 (5 seconds)
      Retry Interval: 5 (5 seconds)
      Expire limit: 2592000 (30 days)
      Minimum TTL: 3600 (1 hour)

```

[\[Request In: 104\]](#)

(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。
答：反复解析图例附在最后。

1. 主机想知道某个域名的 IP 地址，则先去查询浏览器缓存中是否存在，如果存在的话直接返回。
2. 如果浏览器缓存中不存在该域名的 IP 地址，那么继续查询操作系统中是否有该缓存，如果有的话直接返回。如果操作系统缓存中也没有，那么主机向本地域名服务器发送一个 DNS 查询报文，该报文中包含所查询的域名。
3. 如果本地域名服务器缓存有这一 IP 地址的映射，那么就将该 IP 地址返回给请求主机，请求主机再缓存这一映射。如果没有缓存的话，本地域名服务器再将这一请求报文转发给根域名服务器。
4. 根域名服务器不会直接指明这个域名对应的 IP 地址，而是把顶级域名服务器的地址返回给本地域名服务器。
5. 本地域名服务器收到顶级域名服务器地址后，向它发送获取权限域名服务器地址的请求。
6. 收到报文的顶级域名服务器观察其所属的权限域名服务器，并且使用该权限域名服务器的地址做出响应，发回给本地域名服务器。
7. 本地域名服务器再次向该权限域名服务器发出查询报文。
8. 权限域名服务器根据该域名进行查询，用该域名的 IP 地址进行响应，发回给本地域名服务器。本地域名服务器缓存中存入该域名到 IP 地址的映射。
9. 本地域名服务器将该 IP 地址返回给请求主机，请求主机的操作系统再缓存这一映射。
10. 操作系统将这一 IP 地址返回给浏览器，浏览器得到了此 IP 地址，同时放进缓存中。



• DNS 重定向方法:

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

• DNS 重定向过程:

dns 请求当地 local DNS

当地 local DNS 递归的查询服务器的 gslb

服务器根据 local DNS 分配最佳节点，返回 ip

用户获得最佳接入 ip，访问最佳节点。

如果该节点没有用户想要获取的内容，则通过内部路由访问上一节点，直到找到文件或到达源站为止。

cdn 节点缓存该数据，下次请求该文件时可以直接返回。

• 原始记录修改方法

cdn 中缓存了服务器上的部分资源。当服务器去更新 cdn 节点的缓存时，有两种方式，一种是服务器主动去更新缓存，cdn 节点被动接受。另一种方式是当用户请求的资源不存在时，cdn 服务器向上游服务器发起请求，更新缓存，然后将数据返回给用户，这种方式是 cdn 服

务器主动，源站服务器被动。

(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。

答：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问题的数量、回答的数量，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，多人为保证高可用性，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。