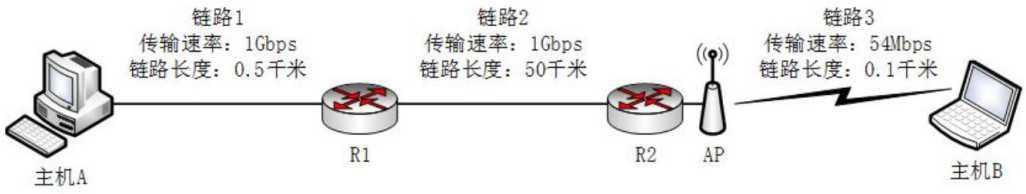
习题 1-1（50 分）

网络的结构如下图所示，主机 A 与主机 B 之间通过 3 段链路和 2 台路由器（R1 与 R2）连接，每条链路的长度和传输速率在图中标出，R1 与 R2 采用存储转发机制，主机 B 向主机 A 发送一个长度为 9000 字节的报文。设电磁波在有线链路与无线链路中的传播速度分别为 2×10^8 米/秒与 3×10^8 米/秒，忽略 R2 与 AP 之间连接使用的链路，忽略报文在 R1 与 R2 的路由决策与排队的延时。



请回答以下 3 个问题：

（1）如果采用报文交换模式，请计算报文传输的最小端到端延时（从主机 B 传输报文第一位开始，到主机 A 接收到报文最后一位所用的时间）（20 分）

(1) 传播时延 + 传输时延

$$= \frac{0.1\times10^3}{3\times10^8} + \frac{50\times10^3}{2\times10^8} + \frac{0.5\times10^3}{2\times10^8} + \frac{9000\times8}{1\times10^3\times10^6}\times2 + \frac{9000\times8}{54\times10^6}$$

$$= 173.02\times10^{-5}\,s$$

$$= 1.7302\,ms$$

报文传输的最小端到端延时为 1.7302ms

（2）如果将报文平均分成 3 个分组依次传输，请计算完成报文传输的最小端到端延时（忽略报文封装成分组的开销）（20 分）

(2) 每个分组 $9000\div3=3000$ 字节

时延 $= \frac{3000\times8}{54\times10^6}\times3 + \frac{0.5\times10^3}{2\times10^8} + \frac{3000\times8}{1000\times10^6} + \frac{50\times10^3}{2\times10^8}$

$$+ \frac{3000\times8}{1000\times10^6} + \frac{0.1\times10^3}{3\times10^8}$$

$$\approx 1.63\,ms$$

报文传输的最小端到端延时为 1.63ms

（3）如果考虑报文在路由器中的路由决策与排队过程，那么端到端延时不确定性的来源及影响最大的因素（10 分）

端到端延时的不确定性主要来源于以下几点：

1.队列排队延时：这是影响最大的因素，取决于路由器的流量负载和拥塞情况。高流量时排队延时会显著增加。

2.路由决策时间：路由器查找路由表并确定转发路径所需的时间，通常较短，但在复杂路由表或高负载情况下可能增加。

3.链路竞争与重传：特别是在无线链路中，冲突和重传会导致延时不确定性。

4.网络动态变化：如拓扑变化或链路拥塞，会导致路径调整或延时波动。

其中，**队列排队延时**是影响延时不确定性的最大因素，因为它直接与流量负载和网络拥塞程度相关，并且在高负载情况下可能出现指数级增长的延时。

习题 1-2（50 分）

通过 Windows 命令行模式下的 nslookup 命令查询 www.163.com，同时打开 Wireshark 软件捕获上述 nslookup 相关的 DNS 报文。

请回答以下 3 个问题：

（1）提供 nslookup 查询结果截图，并对查询结果进行全面分析（20 分）

nslookup 查询结果截图：

```
C:\Users\lenovo>nslookup www.163.com
服务器:  41.45.30.222.in-addr.arpa
Address:  222.30.45.41

非权威应答:
名称:    www.163.com.w.kunluncan.com
Addresses:  2408:8710:1020:fd00:3::3f8
          2408:8710:1020:fd00:3::3f9
          125.39.43.219
          125.39.43.240
          125.39.43.239
          125.39.135.217
          125.39.43.214
          125.39.135.215
          111.161.79.235
          125.39.43.215
          111.161.79.232
          111.161.79.233
          125.39.135.186
          125.39.43.217
          111.161.79.234
          125.39.43.218
          125.39.135.216
          125.39.43.216
Aliases:  www.163.com
          www.163.com.163jiasu.com
```

查询结果分析：

①服务器信息：

执行 DNS 查询时使用的 DNS 服务器是 41.45.30.222.in-addr.arpa（通常是反向 DNS 查找的域名形式），其 IP 地址为 222.30.45.41。

41.45.30.222.in-addr.arpa 这种 DNS 名称看起来与反向查找（即 IP 地址转为域名）相关，可能表示这是一个反向 DNS 解析服务器的响应。

②非权威应答：

说明这是一个中继查询的结果，查询结果并非来自 www.163.com 的权威 DNS 服务器，而是从其他 DNS 服务器获取的缓存信息。

解析结果中的 www.163.com.w.kunluncan.com 表明 www.163.com 可能与域名 w.kunluncan.com 关联，或这个域名被用作某种代理或转发服务。这有时可能是由于 DNS 劫持或中间 DNS 服务器做了某些重定向。

③地址信息：

图中是 www.163.com 解析出的多个 IP 地址。

Pv6 地址：2408:8710:1020:fd00:3::3f8 和 2408:8710:1020:fd00:3::3f9 是 IPv6 地址，显示了该网站也支持通过 IPv6 协议访问。

IPv4 地址：列出了多个 IPv4 地址，包括 125.39.43.219, 125.39.43.240, 125.39.43.239 等。多个 IP 地址表明该域名使用了负载均衡技术，可能分布在不同的服务器或数据中心，提供更好的访问性能和容错性。这些 IP 地址可能属于不同地理区域或网络，进一步优化网站的响应时间和可用性。

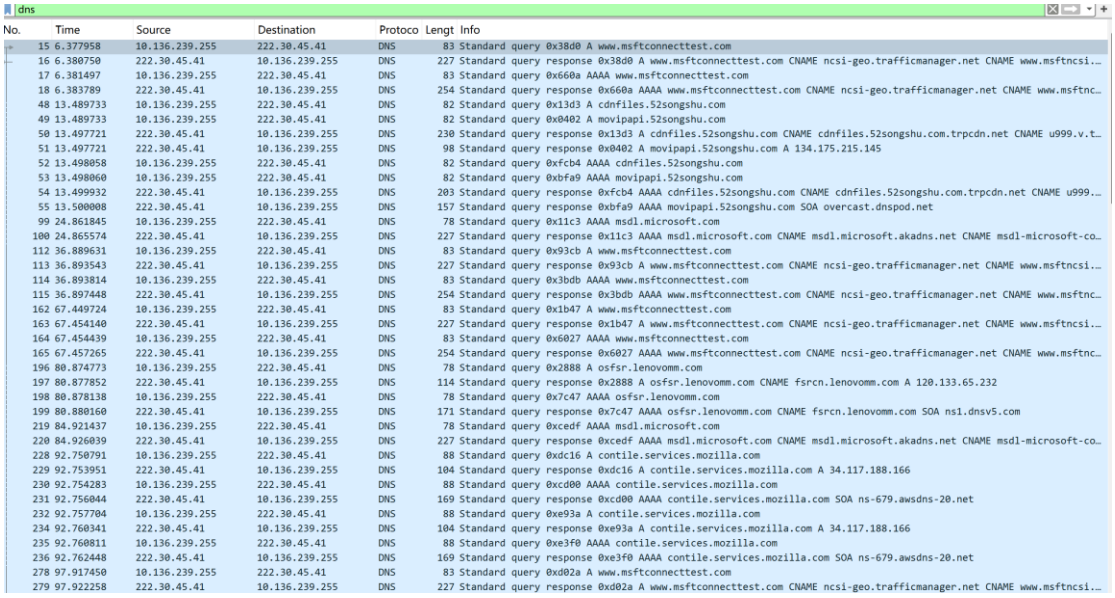
④别名：

www.163.com 有一个别名，指向 www.163.com.163jiasu.com。这种别名通常是由 CNAME 记录（别名记录）实现的，这表示 www.163.com 可能通过一个 CDN（内容分发网络）或代理服务器来实现访问。

通过以上信息我们总结出：

DNS 查询服务器返回的是非权威应答，DNS 服务器可能是一个中继或缓存服务；域名 www.163.com 使用了负载均衡技术，并同时提供 IPv4 和 IPv6 地址；www.163.com 有一个 CNAME 别名，指向 www.163.com.163jiasu.com，可能与 CDN 或代理服务器有关。

（2）提供 Wireshark 捕获结果截图（仅过滤出 DNS 报文），并说明每条 DNS 报文的用途（20 分）



dns

No.	Time	Source	Destination	Protoco	Lengt	Info
15	6.377958	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x38d0 A www.msftconnecttest.com
16	6.380750	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0x38d0 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.…
17	6.381497	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x660a AAAA www.msftconnecttest.com
18	6.383789	222.30.45.41	10.136.239.255	DNS	254	Standard query response 0x660a AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftnc…
48	13.489733	10.136.239.255	222.30.45.41	DNS	82	Standard query 0x13d3 A cdnfiles.52songshu.com
49	13.489733	10.136.239.255	222.30.45.41	DNS	82	Standard query 0x0402 A movipapi.52songshu.com
50	13.497721	222.30.45.41	10.136.239.255	DNS	230	Standard query response 0x13d3 A cdnfiles.52songshu.com CNAME cdnfiles.52songshu.com.trpcdn.net CNAME u999.v.t…
51	13.497721	222.30.45.41	10.136.239.255	DNS	98	Standard query response 0x0402 A movipapi.52songshu.com A 134.175.215.145
52	13.498058	10.136.239.255	222.30.45.41	DNS	82	Standard query 0xfcb4 AAAA cdnfiles.52songshu.com
53	13.498060	10.136.239.255	222.30.45.41	DNS	82	Standard query 0xbfa9 AAAA movipapi.52songshu.com
54	13.499932	222.30.45.41	10.136.239.255	DNS	203	Standard query response 0xfcb4 AAAA cdnfiles.52songshu.com CNAME cdnfiles.52songshu.com.trpcdn.net CNAME u999.…
55	13.500008	222.30.45.41	10.136.239.255	DNS	157	Standard query response 0xbfa9 AAAA movipapi.52songshu.com SOA overcast.dnspod.net
99	24.861845	10.136.239.255	222.30.45.41	DNS	78	Standard query 0x11c3 AAAA msdl.microsoft.com
100	24.865574	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0x11c3 AAAA msdl.microsoft.com CNAME msdl.microsoft.akadns.net CNAME msdl-microsoft-co…
112	36.889631	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x93cb A www.msftconnecttest.com
113	36.893543	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0x93cb A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.…
114	36.893814	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x3bdb AAAA www.msftconnecttest.com
115	36.897448	222.30.45.41	10.136.239.255	DNS	254	Standard query response 0x3bdb AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftnc…
162	67.449724	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x1b47 A www.msftconnecttest.com
163	67.454140	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0x1b47 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.…
164	67.454439	10.136.239.255	222.30.45.41	DNS	83	Standard query 0x6027 AAAA www.msftconnecttest.com
165	67.457265	222.30.45.41	10.136.239.255	DNS	254	Standard query response 0x6027 AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftnc…
196	80.874773	10.136.239.255	222.30.45.41	DNS	78	Standard query 0x2888 A osfsr.lenovomm.com
197	80.877852	222.30.45.41	10.136.239.255	DNS	114	Standard query response 0x2888 A osfsr.lenovomm.com CNAME fsrcn.lenovomm.com A 120.133.65.232
198	80.878138	10.136.239.255	222.30.45.41	DNS	78	Standard query 0x7c47 AAAA osfsr.lenovomm.com
199	80.880160	222.30.45.41	10.136.239.255	DNS	171	Standard query response 0x7c47 AAAA osfsr.lenovomm.com CNAME fsrcn.lenovomm.com SOA ns1.dnsv5.com
219	84.921437	10.136.239.255	222.30.45.41	DNS	78	Standard query 0xcedf AAAA msdl.microsoft.com
220	84.926039	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0xcedf AAAA msdl.microsoft.com CNAME msdl.microsoft.akadns.net CNAME msdl-microsoft-co…
228	92.750791	10.136.239.255	222.30.45.41	DNS	88	Standard query 0xdc16 A contile.services.mozilla.com
229	92.753951	222.30.45.41	10.136.239.255	DNS	104	Standard query response 0xdc16 A contile.services.mozilla.com A 34.117.188.166
230	92.754283	10.136.239.255	222.30.45.41	DNS	88	Standard query 0xcd00 AAAA contile.services.mozilla.com
231	92.756044	222.30.45.41	10.136.239.255	DNS	169	Standard query response 0xcd00 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
232	92.757704	10.136.239.255	222.30.45.41	DNS	88	Standard query 0xe93a A contile.services.mozilla.com
234	92.760341	222.30.45.41	10.136.239.255	DNS	104	Standard query response 0xe93a A contile.services.mozilla.com A 34.117.188.166
235	92.760811	10.136.239.255	222.30.45.41	DNS	88	Standard query 0xe3f0 AAAA contile.services.mozilla.com
236	92.762448	222.30.45.41	10.136.239.255	DNS	169	Standard query response 0xe3f0 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
278	97.917450	10.136.239.255	222.30.45.41	DNS	83	Standard query 0xd02a A www.msftconnecttest.com
279	97.922258	222.30.45.41	10.136.239.255	DNS	227	Standard query response 0xd02a A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.…

• 报文 15

用途:标准查询报文，请求解析域名 www.msftconnecttest.com 的 A 记录，即查询目标域名的 IPv4 地址。

这是典型的域名解析查询报文，用户向 DNS 服务器发送请求，期望获得目标域名对应的 IPv4 地址。此类报文常用于确定服务器的网络位置。

• 报文 16

用途:这是 DNS 服务器返回的响应报文，包含 www.msftconnecttest.com 的 A 记录查询结果。

服务器成功解析了目标域名，并将对应的 IPv4 地址返回给客户端，完成一次完整的 DNS 查询过程。

• 报文 17

用途:这是一个 DNS 查询报文，客户端向 DNS 服务器请求解析 www.msftconnecttest.com 的 AAAA 记录（IPv6 地址）。

客户端尝试获取目标域名的 IPv6 地址。如果支持 IPv6，客户端可能优先使用 IPv6 建立连接。

• 报文 18

用途:这是 DNS 服务器返回的响应报文，包含 www.msftconnecttest.com 的 AAAA 记

录 查询结果。

服务器返回了目标域名的 IPv6 地址（如果有），或者表示该域名不支持 IPv6。

• 报文 45

用途:标准查询报文，请求解析域名 4.cnfiles.52songshu.com 的 A 记录。

这是另一个域名的解析请求，目的是获取该域名的 IPv4 地址。此类报文通常是因为用户访问某些网站时，涉及第三方资源（如广告、服务请求）的域名解析。

• 报文 47

用途:DNS 服务器返回域名 4.cnfiles.52songshu.com 的解析结果（A 记录）。

DNS 服务器将解析到的 IPv4 地址返回给客户端，表示该域名的解析成功。客户端会使用返回的地址与目标服务器通信。

• 报文 51

用途:标准查询报文，请求解析域名 4.cnfiles.52songshu.com 的 AAAA 记录。

这条报文是针对 4.cnfiles.52songshu.com 的 IPv6 地址（AAAA 记录）进行查询。如果服务器支持 IPv6，客户端可能优先使用 IPv6 地址。

• 报文 73

用途:标准查询报文，请求解析域名 fsrcn.lenovomm.com 的 A 记录。

该报文表明用户尝试访问 Lenovo 的某项服务，DNS 查询请求目标是获取 fsrcn.lenovomm.com 的 IPv4 地址。

• 报文 77

用途:DNS 服务器返回域名 fsrcn.lenovomm.com 的解析结果（A 记录）。

这是针对前一条报文的响应，DNS 服务器返回了 fsrcn.lenovomm.com 的 IPv4 地址。客户端随后会使用该地址进行数据交互。

• 报文 231

标准查询报文，请求解析域名 contile.services.mozilla.com 的 A 记录。

用户访问 Mozilla 的服务时需要进行域名解析，查询目标是获取该服务的 IPv4 地址。

•报文 233：DNS 服务器返回域名 contile.services.mozilla.com 的解析结果（A 记录）。

这是 DNS 服务器解析的响应结果，返回目标域名的 IPv4 地址。客户端随后会使用解析到的地址与目标服务器建立连接。

• 报文 279

用途:查询 www.msftconnecttest.com 的 CNAME 记录 和 A 记录。

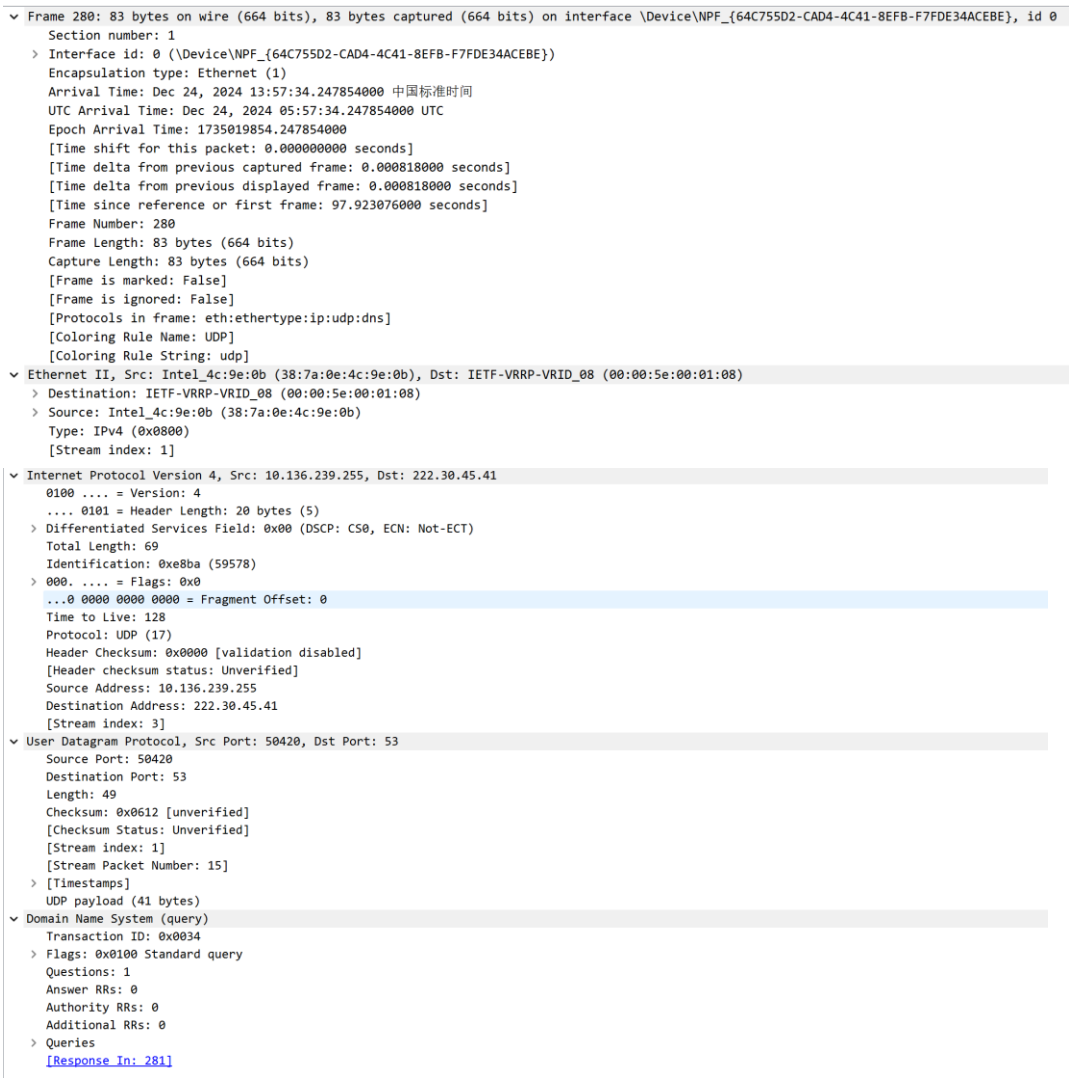
这是一个组合查询，既请求目标域名的 CNAME（别名记录），也请求其 A 记录（IPv4 地址）。如果域名设置了别名，CNAME 会指向最终的目标地址。返回的 A 记录表示实际使用的 IPv4 地址。

通过分析以上 DNS 报文，可以归纳其用途为以下几点：

① 查询报文:责向 DNS 服务器请求解析域名，返回域名对应的 IP 地址或别名。查询类型包括：A 记录（IPv4 地址）；AAAA 记录（IPv6 地址）；CNAME 记录（别名记录）。

② 响应报文:负责从 DNS 服务器返回查询结果，供客户端使用。如果查询成功，则返回目标域名的 IP 地址；如果失败，则返回错误信息或 NXDOMAIN（域名不存在）。

（3）提供某个 DNS 报文详细信息截图，说明 DNS 服务使用哪种传输层协议，以及哪些措施可提高 DNS 服务可靠性（10 分）



DNS 服务在这次查询中使用了 **UDP** 作为传输层协议。

以下措施可提高 DNS 服务可靠性：

1.部署主从 DNS 服务器：配置多台 DNS 服务器（主服务器和从服务器）以防止单点故障。当主服务器无法工作时，从服务器可以继续提供域名解析服务。例如，在权威 DNS 配置中，可以使用多个 NS 记录（Name Server）来定义多台权威服务器。

2.启用 DNS 缓存：在客户端和本地 DNS 服务器中启用缓存，减少对权威 DNS 服务器的直接查询压力。DNS 缓存可以提高查询速度，并降低网络延迟。同时可以设置合理的 TTL（生存时间）值，确保缓存信息及时更新，避免陈旧数据影响解析。

3.使用负载均衡和地理分布式 DNS：通过负载均衡将查询分散到多个 DNS 服务器，防止某一台服务器因流量过载而宕机。部署地理分布式的 DNS 服务器，让用户访问离自己最近的 DNS 节点，减少延迟并提高服务响应速度。

4.DNSSEC（DNS Security Extensions）：实施 DNSSEC 来增强 DNS 数据的完整性和真实性，防止攻击者篡改解析结果（如 DNS 劫持）。通过数字签名验证 DNS 数据的来源，确保查询返回的记录是权威可信的。

5.启用 Anycast 技术：使用 Anycast 将同一个 DNS IP 地址广播到多个服务器，用户的查询会自动路由到最近或最快的服务器。提高容灾能力，当某个节点故障时，流量会自动切换到其他节点。

6.定期监控和健康检查：对 DNS 服务器的运行状态进行实时监控，发现问题及时修复。设置健康检查机制，自动检测服务器的可用性，失效时快速切换到备用服务器。

7.保护 DNS 服务器的安全性：限制不必要的开放端口，只允许必要的 DNS 流量通过。配置防火墙规则，防止未经授权的访问。实施防 DDoS（分布式拒绝服务）攻击的措施，例如启用 DDoS 防护服务。

8.支持 DoH（DNS over HTTPS）或 DoT（DNS over TLS）：通过加密 DNS 查询，保护用户隐私，防止 DNS 数据被窃听或篡改。DoH 使用 HTTPS 协议，DoT 使用 TLS 协议，这两种方式均可提高 DNS 查询的安全性。

9.合理的超时设置：在 DNS 查询中设置合理的超时时间（Timeout），防止查询长时间等待无响应。结合重试机制，当某台服务器失效时，快速切换到其他服务器查询。

10.冗余网络连接：为 DNS 服务器配置冗余的网络路径，避免网络单点故障影响解析服务的可用性。使用多个 ISP 提供商，确保网络的多路径连接性。