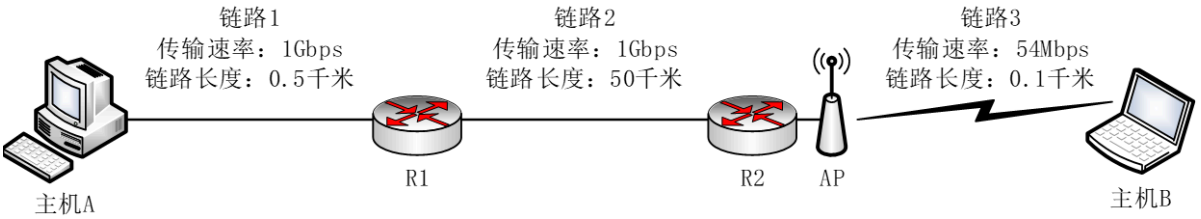
《计算机网络》书面作业-1

学院：网络空间安全学院　专业：信息安全　姓名：陆皓喆

习题1-1

题目

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)

(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)

(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)

解答

(1)从主机B传输到主机A，需要经过三段链路，其中第一段为无线链路，后面两段为有线链路。

最小端到端延时为数据部分的传输时间，加上在链路上的传播时延。

$$T=\frac{9000\times8}{54\times10^6}+\frac{0.1\times1000}{3\times10^8}+\frac{9000\times8}{1\times10^9}+\frac{50000}{2\times10^8}+\frac{9000\times8}{1\times10^9}+\frac{0.5\times1000}{2\times10^8}$$

计算得到：

$$T=1730.16\times10^{-6}s\approx1.73ms$$

答：报文传输的最小端到端延时为$1.73ms$

(2)这一问，和第一问的变化就是，将报文分成了三组进行传输。我们只需要修改一下每一段的报文长度即可，修改为3000字节。

我们计算一下单个分组内各部分的传输时间。

第一组报文的传输时间：

$$T_1=\frac{3000\times8}{54\times10^6}\approx4.44\times10^{-4}$$

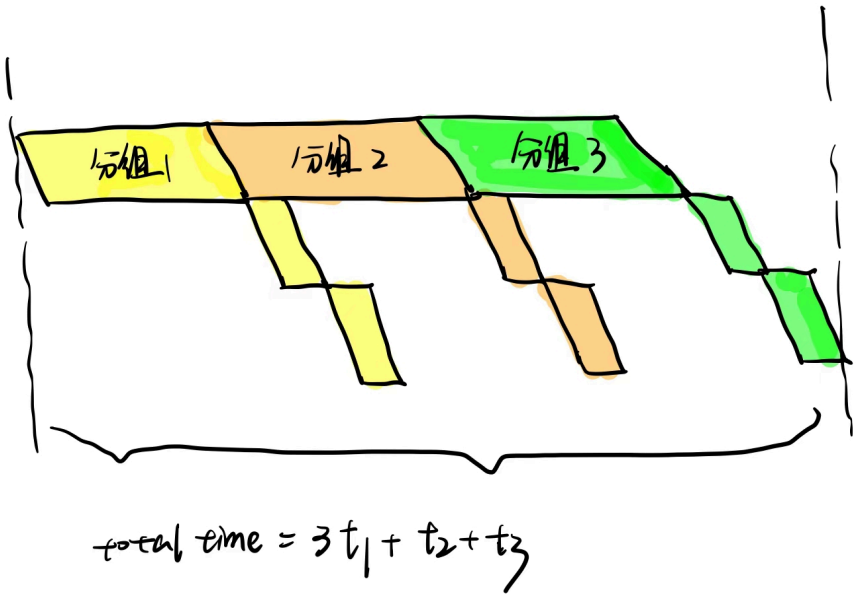
第二段报文的传输时间+传播时延：

$$T_2 = \frac{3000 \times 8}{1 \times 10^9} + \frac{50000}{2 \times 10^8} \approx 2.74 \times 10^{-4}$$

发现：

$$T_1 > T_2$$

我们发现，当第二段到达目的地的时候，第一段的下一个分组还没有到达，所以实际上我们可以把第一段链路算三倍时间，后面两段链路只需要算一次就可以。大致的传播流水线图如下所示：



所以可以列出式子：

$$T = \frac{3000 \times 8}{54 \times 10^6} \times 3 + \frac{0.1 \times 1000}{3 \times 10^8} + \frac{3000 \times 8}{1 \times 10^9} + \frac{50000}{2 \times 10^8} + \frac{3000 \times 8}{1 \times 10^9} + \frac{0.5 \times 1000}{2 \times 10^8}$$

计算得到：

$$T = 1634.16 \times 10^{-6} s \approx 1.634 ms$$

答：报文传输的最小端到端延时为$1.634ms$

(3)

端到端延时不确定性的来源：

- 转发设备中的排队延时
- 转发设备中的处理时间：路由决策、差错检验、分片等操作
- 分组大小和分组数量、数据流的个数、数据流占带宽的频率
- 链路传输的速率与链路的长度

影响最大的因素：转发设备中的排队延时

习题1-2

题目

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)

(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)

(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)

解答

(1)**查询结果截图如下所示：**

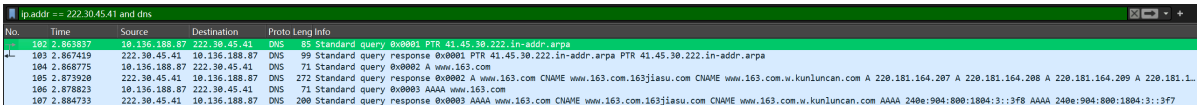
```
PS E:\学学学\本科\大三上\计算机网络\homework\homework1> nslookup www.163.com
Server:  41.45.30.222.in-addr.arpa
Address:  222.30.45.41

Non-authoritative answer:
Name:    www.163.com.w.kunluncan.com
Addresses:  240e:904:800:1804:3::3f8
          240e:904:800:1804:3::3f7
          220.181.164.204
          220.181.164.203
          220.181.164.206
          220.181.164.205
          220.181.164.210
          220.181.164.207
          220.181.164.209
          220.181.164.208
Aliases:  www.163.com
          www.163.com.163jiasu.com
```

查询结果分析：

- `Server: 41.45.30.222.in-addr.arpa`:这是我的本地DNS服务器的域名；
- `Address: 222.30.45.41`:这是我的本地DNS服务器的$ipv4$地址；
- `Non-authoritative answer:`:这一行代表了，我们的查询信息是从非权威DNS服务器或者是从本地缓存中检索得到的，这样的应答就叫做非权威应答。如果是权威应答的话，就说明我们的信息是从当前区域的权威服务器所查询得到的；
- `Name: www.163.com.w.kunluncan.com`:这一行代表了我们查询到的确切的域名，也就是`www.163.com.w.kunluncan.com`，这是我们的规范主机名；
- $Addresses$中列举出了与这个域名相关联的IP地址，其中包括了多个ip地址，包括两个$ipv6$地址和八个$ipv4$地址；
- `Aliases:`最后列举出了目标域名的一些别名，包括了`www.163.com`和`www.163.com.163jiasu.com`

(2)

我们首先使用ip地址和DNS特征对捕获内容进行过滤，**得到了$Wireshark$捕获截图**：



从上到下，共捕获到六条DNS报文。其中源IP和目的IP分别为主机IP与本地$DNS\ Server$的IP

每条DNS报文的用途：

1. 第一条DNS报文的作用是：本机向本地的DNS进行反向的域名解析
2. 第二条DNS报文的作用是：回复对应的域名，`41.45.30.222.in-addr.arpa`
3. 第三条DNS报文的作用是：本机请求`www.163.com`的$ipv4$地址
4. 第四条DNS报文的作用是：返回了八个对应的$ipv4$地址以及规范主机名和别名，和前面的查询结果是相同的
5. 第五条DNS报文的作用是：本机请求`www.163.com`的$ipv6$地址
6. 第六条DNS报文的作用是：返回了两个对应的$ipv6$地址以及规范主机名和别名，和前面的查询结果是相同的

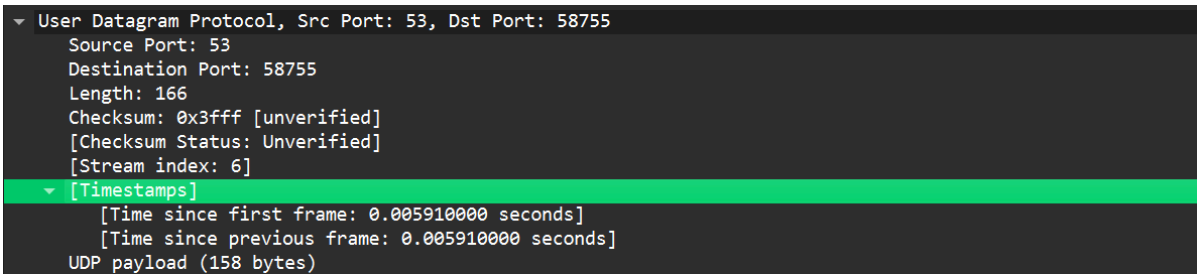
(3)我们以上一问中的第六条报文举例子说明。

报文截图如下所示：

```
Domain Name System (response)
    Transaction ID: 0x0003
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.163.com: type AAAA, class IN
        Name: www.163.com
        [Name Length: 11]
        [Label Count: 3]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  ▾ Answers
    ▸ www.163.com: type CNAME, class IN, cname www.163.com.163jiasu.com
    ▸ www.163.com.163jiasu.com: type CNAME, class IN, cname www.163.com.w.kunluncan.com
    ▾ www.163.com.w.kunluncan.com: type AAAA, class IN, addr 240e:904:800:1804:3::3f8
        Name: www.163.com.w.kunluncan.com
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 64 (1 minute, 4 seconds)
        Data length: 16
        AAAA Address: 240e:904:800:1804:3::3f8
    ▾ www.163.com.w.kunluncan.com: type AAAA, class IN, addr 240e:904:800:1804:3::3f7
        Name: www.163.com.w.kunluncan.com
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 64 (1 minute, 4 seconds)
        Data length: 16
        AAAA Address: 240e:904:800:1804:3::3f7
    [Request In: 106]
    [Time: 0.005910000 seconds]
```

可以看到，本机向目标域名发出了请求，请求其$ipv6$地址；目标域名做了应答，返回了两个$ipv6$地址，和前面的查询结果相同。

从下图中，我们可以看到，DNS服务采用了UDP传输层协议，使用了53号端口。



提高DNS服务可靠性的措施：

- 我们的DNS可靠性由UDP来进行保证，如上图中的$checksum$，就是UDP的差错检测功能。为了提高DNS服务器可靠性，我们可以使用TCP协议，通过ACK确认、差错检测、滑动窗口机制、流量控制、拥塞控制等功能来提高DNS的可靠性；
- 我们还可以部署一些DNS冗余服务器，部署多台DNS主服务器，在不同的地区进行设置，避免单点故障；
- 我们还可以对其进行缓存优化。可以通过合理设置TTL，或者使用递归查询缓存的方式来进行优化；
- 我们还可以启用$DNS\ cookie$进行验证，加强安全性；