一、简答

1. 以太网的最大最小帧长，为什么要有？

答：以太网的最大帧长为 1500 字节，其存在的原因是：①如果帧长过长，会造成接收端的缓存溢出，发生错误；②由于以太网是多个主机共享媒介信道，如果帧长过长，也将导致某一主机占据信道过久，不公平。

以太网的最小帧长需根据实际往返时间而定，一般至少为 46 字节。如果帧长过短，会导致在 CSMA/CD 中无法检测出碰撞，所以要求发送帧的最短时间 TXT 要大于链路最大的往返时间 RTT，根据链路的带宽，可计算出最小帧长。

2. 802.3 和 802.11 协议的异同

答：802.3 链路层以太网的协议，802.11 为无线局域网中的协议。

相同点：两者均是链路层局域网标准，都是基于 MAC 地址寻址的。在多路访问中，均采用了载波侦听 CSMA 的形式。

不同点：

① 802.3 是基于有线网络，而 802.11 是基于无线网络。

② 在多路访问中，802.3 提供了 CD 碰撞检测机制，检测到碰撞后随机回退；802.11 提供了 CA 碰撞避免机制。

③ 在 802.11 中，由于无线信道衰减强切易受干扰，所以还提供了链路层确认/重传 ARQ 机制，提供可靠的连接服务；在 802.3 中只是检测帧是否损坏，属于不可靠的无连接服务。

④ 802.3 是基于以太网帧，有两个 MAC 地址；802.11 是基于 802.11 帧，3 个 MAC 地址机制。

3. Rdt3.0 提供了哪些可靠的服务？

① 校验和位差检测，错误重传

② 丢弃冗余数据

③ 允许 ACK 出错、重复分组，设置序号

④ 允许数据丢失，设置超时时间，超时重传

4. IPv6 和 IPv4 的区别？前者的偏移地址是多少位？报头格式？

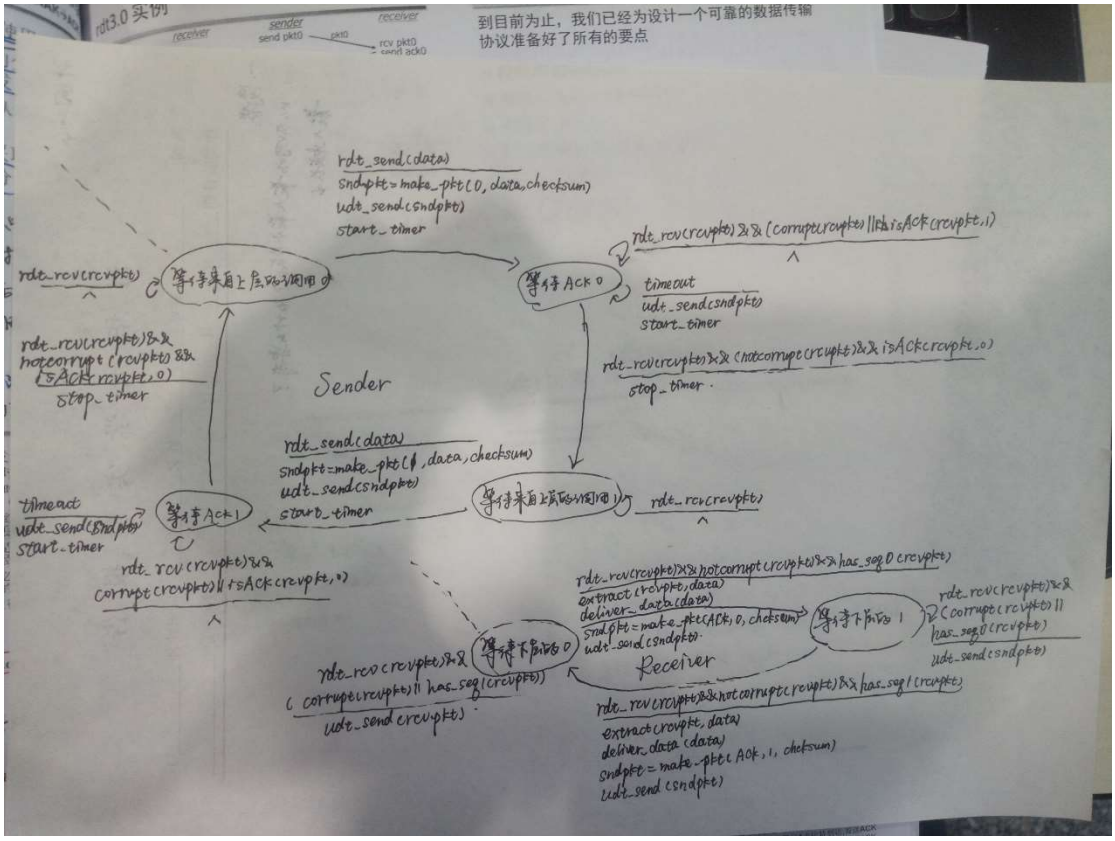
答：

区别：IPv6 的地址为 128 位，IPv4 的地址为 32 位。IPv6 层次化分配 IP 地址，地址空间较大。IPv6 的报头长度固定为 40 字节，IPv4 报头长度一般为 20 字节，但不固定，可能达到 60 字节。IPv6 没有 checksum，没有分片机制，而是增加了优先级域和流标记域来保证服务质量。

IPv6 的偏移地址没有，IPv4 的偏移地址为 13 位。

报头格式：IPv6 的报头长度固定为 40 字节，IPv4 报头长度一般为 20 字节，但不固定，可能达到 60 字节。IPv6 没有 checksum，没有分片机制，而是增加了优先级域和流标记域来保证服务质量。

二、画出 rdt3.0 的 FSM 流程图



三、N=4，编号为 0，1，2，3，…，10，发送几个分组的时延为 2RTT，定时重传时延为 0.4RTT.

1. GBN：只有分组 2 在发送时丢失，求接下来 N 个发送分组的编号

   先发分组 0,1,2,3；返回 ACK0,1；定时器开启；发送窗口移动为 2345；发送分组 4,5；但分组 3,4,5 被接收方丢弃；ACK1 冗余被发送方丢弃；等不到 ACK2；发送方超时重发分组 2；

   如果定时时延较大，则顺序为分组 0,1,2,3,4,5,2,3,4,5,6,7,8,9,10

2. SR：只有分组 2 在发送时丢失，求接下来 N 个发送分组的编号

   先发分组 0,1,2,3；返回 ACK0,1,3；发送分组 2 时，分组 2 的定时器开启；发送窗口移动为 2345;发送分组 4,5;接收方接收分组 4,5,并缓存,返回 ACK4,5;但发送方在等 ACK2，没有等到；分组 2 的定时器超时，重传分组 2；

   如果定时时延较大，则顺序为分组 0,1,2,3,4,5,2,,6,7,8,9,10

3. TCP RENO 发送 0 丢失后，估算下一次重发的时间，写出两个编号

   发送 0 丢失后，会发生超时 timeout，将 threshold 置为 Congwin/2，并将 Congwin 置为 1。等待超时时间之后即可重发。

四、HTML 文件，大小为 10kBYTEs；还有 10 个 1kBYTEs 的图片。链路带宽为 10Mbps。

1. 非持久 HTTP 响应时间

   HTML 文件的传输时间为 8ms，记为 T1。一个图片的传输时间为 0.8ms，记为 T2。

   则 2RTT+T1+10（2RTT+T2）=22RTT+T1+10T2=22RTT+16ms

2. 非持久、5 个并行 TCP 响应时间

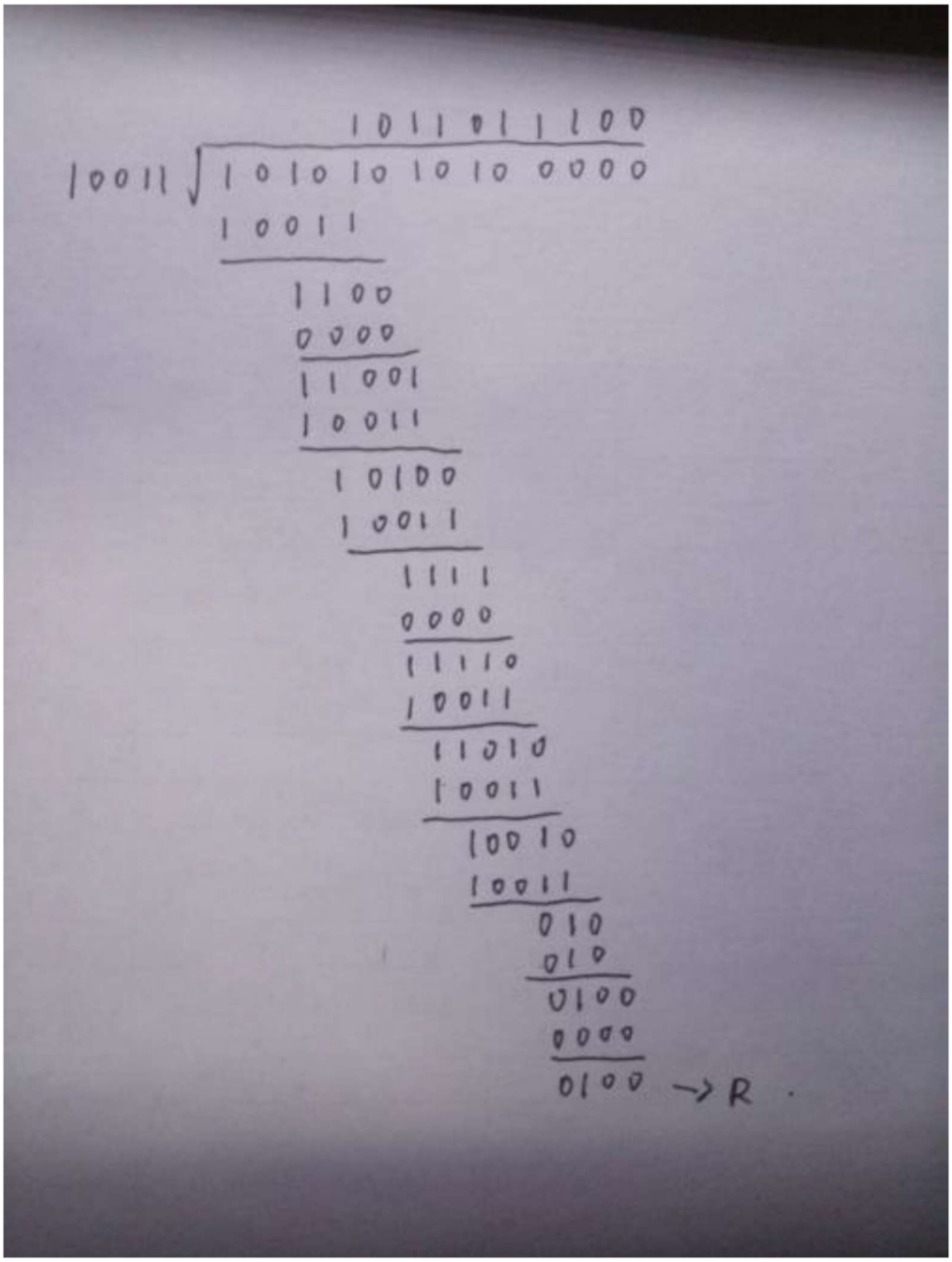
HTML 文件的传输时间为 8ms，记为 T1。5 张图片并行的传输时间为 4ms，记为 T3。
则 2RTT+T1+2(2RTT+T3)=6RTT+16ms

3. 带流水线

HTML 文件的传输时间为 8ms，记为 T1。10 张图片并行的传输时间为 8ms，记为 T3。
则 2RTT+T1+RTT+T3=3RTT+16ms

五、循环冗余检测，给定 D,G，求 R

不妨设 D=1010101010，G=10011
则 R 为 4 位，r=4。



六、主机访问 www.sina.com 所需用到的协议

应用层协议为 DNS 和 HTTP，即除了 HTTP 之外还需要 DNS 协议；
传输层协议为 UDP 和 TCP。
DNS 用于将服务器主机名解析成 IP 地址；
HTTP 协议实现超文本的传输，是 Web 的应用层协议；
TCP：为应用层的协议提供面向连接的可靠传输，即为 HTTP 协议提供可靠的传输服务；
UDP：为应用层协议提供不可靠的传输，其中本题的 DNS 协议需要 UDP 的服务。
IP 协议：在网络层将数据报交付给服务器主机
ARP 协议：将 IP 地址解析为 MAC 地址

1. 若 DNS 缓存中没有相关数据，则 IE 浏览器先向 DNS 服务器发出 DNS 请求；
2. 这一过程的目的是获取 www.sina.com 这个域名所对应的 IP 地址；
3. IE 浏览器向本机 DNS 模块发出 DNS 请求，DNS 模块生成相关的 DNS 报文；
4. DNS 模块将生成的 DNS 报文传递给传输层的 UDP 协议单元；
5. UDP 协议单元将该数据封装成 UDP 数据报，传递给网络层的 IP 协议单元；
6. IP 协议单元将该数据封装成 IP 数据包，其中目的 IP 地址为 DNS 服务器的 IP 地址；
7. 封装好的 IP 数据包将传递给数据链路层的协议单元进行发送；
8. 发送时如果 ARP 缓存中没有相关数据，则发送 ARP 广播请求，等待 ARP 回应；
9. 得到 ARP 回应后，将 IP 地址与路由下一跳 MAC 地址对应的信息写入 ARP 缓存表；
10. 写入缓存后，以路由下一跳地址填充目的 MAC 地址，并以数据帧形式转发；
11. 这个转发过程可能会进行多次，这取决于 DNS 服务器在校园网中的位置；
12. DNS 请求被发送到 DNS 服务器的数据链路层协议单元；
13. DNS 服务器的数据链路层协议单元解析收到的数据帧，将其内部所含有的 IP 数据包传递给网络层 IP 协议单元；
14. DNS 服务器的 IP 协议单元解析收到的 IP 数据包，将其内部所含有的 UDP 数据报传递给传输层的 UDP 协议单元；
15. DNS 服务器的 UDP 协议单元解析收到的 UDP 数据包，将其内部所含有的 DNS 报文传递给该服务器上的 DNS 服务单元；
16. DNS 服务单元收到 DNS 请求，将域名解析为对应的 IP 地址，产生 DNS 回应报文；
17. （所有应用层报文必须通过传输层、网络层和数据链路层，因此在下面的叙述中，我将简化这一过程的叙述，简化形式如下面的样子，其中单箭头为本机内部传递，双箭头为网络上的发送）
18. DNS 回应报文→UDP→IP→MAC→→请求域名解析的主机；
19. 请求域名解析的主机收到数据帧，该数据帧→IP→UDP→DNS→IE 浏览器；
20. 将域名解析的结果以域名和 IP 地址对应的形式写入 DNS 缓存表。

21. IE 浏览器向 www.sina.com.cn 发出 TCP 连接请求报文；
22. 该请求 TCP 报文中的 SYN 标志位被设置为 1，表示连接请求；
23. 该 TCP 请求报文→IP(DNS)→MAC(ARP)→→校园网关→→www.sina.com.cn 主机；
24. 该 TCP 请求报文经过 IP 层时，填入的目的 IP 地址就是上面 DNS 过程获得的 IP 地址；
25. 经过数据链路层时，若 MAC 地址不明，还要进行上面所叙述的 ARP 过程；
26. www.sina.com.cn 收到的数据帧→IP→TCP，TCP 协议单元会回应请求应答报文；
27. 该请求应答 TCP 报文中的 SYN 和 ACK 标志位均被设置为 1，表示连接请求应答；
28. 该 TCP 请求应答报文→IP→MAC(ARP)→→校园网关→→请求主机；
29. 请求主机收到数据帧→IP→TCP，TCP 协议单元会回应请求确认报文；
30. 该请求应答 TCP 报文中的 ACK 标志位被设置为 1，表示连接请求确认；
31. 该 TCP 请求确认报文→IP→MAC(ARP)→→校园网关→→www.sina.com.cn 主机；
32. www.sina.com.cn 收到的数据帧→IP→TCP，连接建立完成；
33. IE 浏览器向 www.sina.com.cn 发出 HTTP-GET 方法报文；
34. 该 HTTP-GET 方法报文→TCP→IP→MAC→→校园网关→→www.sina.com.cn 主机；
35. www.sina.com.cn 收到的数据帧→IP→TCP→HTTP，HTTP 协议单元会回应 HTTP 协议格式封装好的 HTML 超文本形式数据；
36. HTTP-HTML 数据→TCP→IP→MAC(ARP)→→校园网关→→请求主机；
37. 请求主机收到的数据帧→IP→TCP→HTTP→IE 浏览器，浏览器会以网页形式显示 HTML 超文本，就是我们所看到的网页。
38. IE 浏览器向 www.sina.com.cn 发出 TCP 连接结束请求报文；
39. 该请求 TCP 报文中的 FIN 标志位被设置为 1，表示结束请求；
40. 该 TCP 结束请求报文→IP→MAC(ARP)→→校园网关→→www.sina.com.cn 主机；
41. www.sina.com.cn 收到的数据帧→IP→TCP，TCP 协议单元会回应结束应答报文；
42. 该结束应答 TCP 报文中的 FIN 和 ACK 标志位均被设置为 1，表示结束应答；
43. 该 TCP 结束应答报文→IP→MAC(ARP)→→校园网关→→请求主机；

七、路由算法，同往年题

八、求时隙/纯 ALOHA 最优效率 E*下的 p*

1. 时隙 ALOHA

时隙 ALOHA 假设把时间分成相等大小的时隙（等于发送一帧的时间），节点仅在时隙的开始时刻发送帧，各节点是同步的，每个节点知道时隙何时开始，每个节点在每个时隙都以概率 p 发送一帧。所以当某一节点在某时刻发生成功，意味着其他节点在该时隙没有发送，

则有$\mathrm{E(p)} = \mathrm{Np}(1-p)^{N-1}$。

对上式进行求导:

有

$$\mathrm{E'(p)} = \mathrm{N}(1-p)^{N-1} - \mathrm{Np}(N-1)(1-p)^{N-2}$$
$$= \mathrm{N}(1-pN)(1-p)^{N-2}$$

令$\mathrm{E'(p)} = 0$

得到$p^* = \frac{1}{N}$

将$p^* = \frac{1}{N}$代入$\mathrm{E(p)} = \mathrm{Np}(1-p)^{N-1}$中，可以得到:

$$\mathrm{E}(p^*) = \mathrm{N}p^*(1-p^*)^{N-1} = \frac{(1-1/N)^N}{1-1/N}$$

而当 N 趋近于正无穷时，有$\lim_{N\to\infty}(1-1/N)^N = 1/e$，$\lim_{N\to\infty}(1-1/N) = 1$。

从而 $\mathrm{E}(p^*) = 1/e$，即当 N 趋于无穷大时的时隙 ALOHA 的效率为 1/e。

2. 纯 ALOHA

纯 ALOHA 没有假设时隙，假设总共有 N 个节点，某节点在时刻 t 传输信息的概率为 p，而没有其他节点在[t-1,t]时间区间上传送信息的概率为$(1-p)^{N-1}$，没有其他节点在[t,t+1]时间区间上传送信息的概率为$(1-p)^{N-1}$，所以该节点传输成功的概率是$\mathrm{p}(1-p)^{2N-2}$，则纯 ALOHA 系统的效率为$\mathrm{Np}(1-p)^{2N-2}$。

对上式求导，并令导数为 0，可得$p^* = \frac{1}{2N-1}$，代入上式可得

$$\mathrm{N}\frac{1}{2N-1}(1-\frac{1}{2N-1})^{2N-2} \le \frac{1}{2e}$$

当 N 趋近于正无穷时，上式趋近于取等。