原创：<https://www.pianshen.com/article/7992419624/>

https://blog.csdn.net/weixin\_41357767/category\_8842473.html

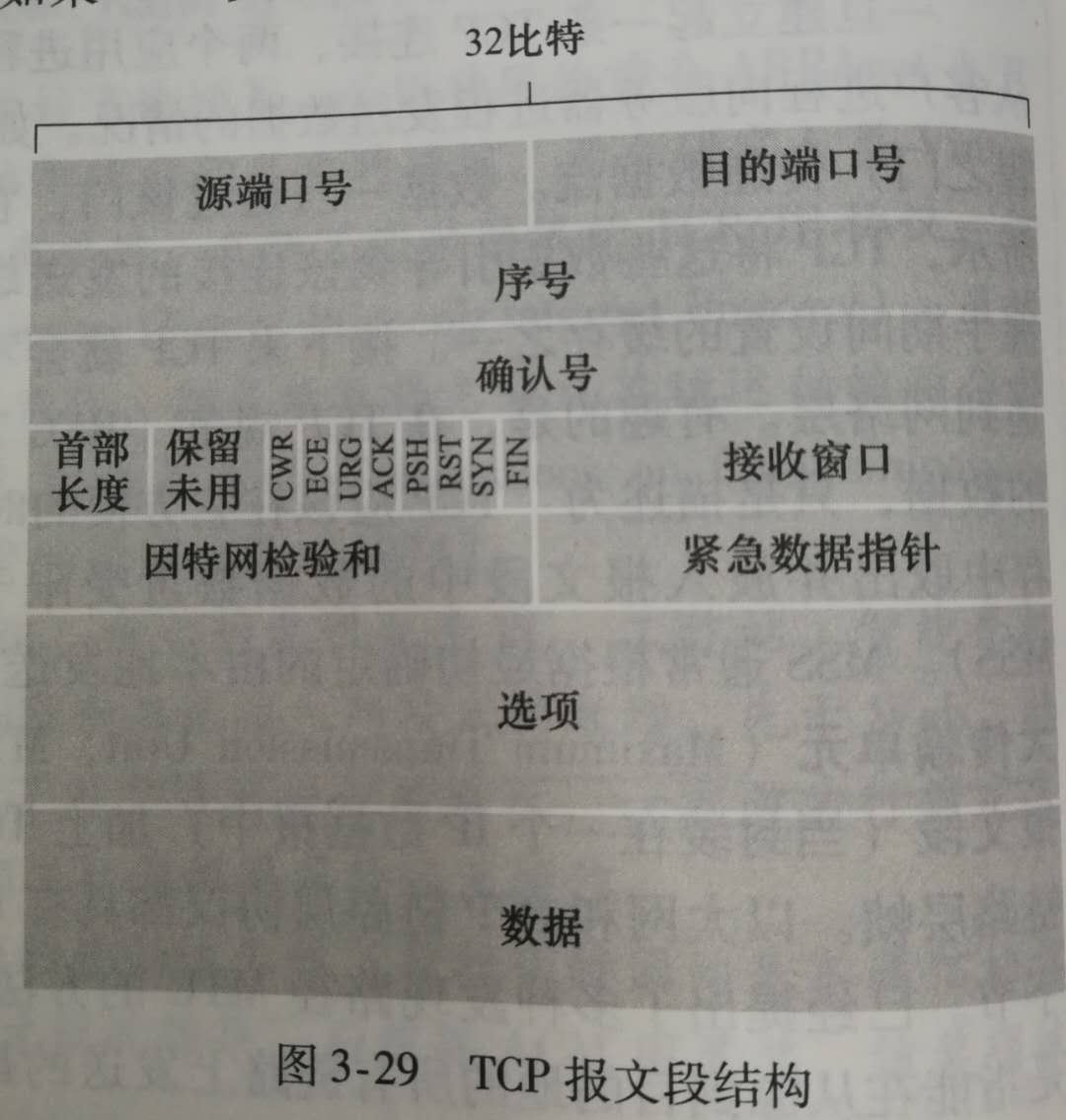
最厉害的是他的TCP总结：

3.4节讲的是如何从零创建起一个可靠高效的数据传输协议。而3.5节基于3.4节的基础具体讲述TCP的实现，这里有必要进行一个简单的总结

注：目前想总结的有第一章计算机网络和因特网、第三张运输层、第四章网络层：数据平面

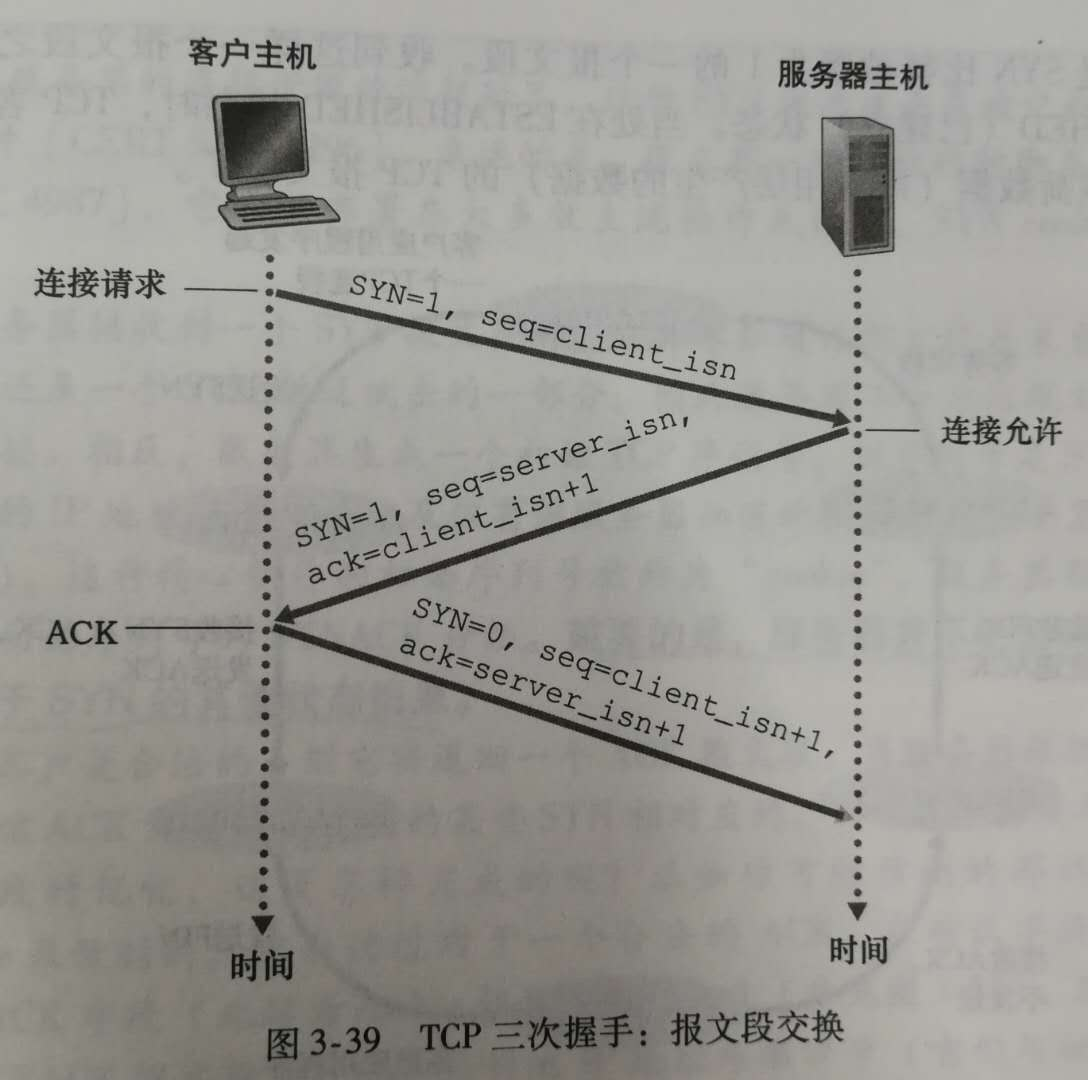
## 一、TCP三次握手

在讲述三次握手之前先看看TCP报文段



对于三次握手问题，我们暂时不考虑报文段中的其他字段，只看报文段中序号和确认序号字段。对这两个字段有印象后，下面开始描述一次完整的TCP三次握手过程

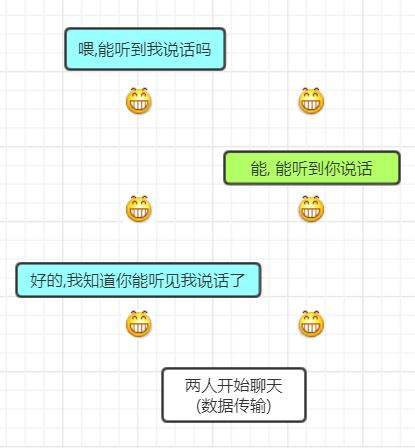
开始



1. 第一步：客户端的TCP向服务器的TCP发送一个特殊的TCP报文段，该报文段不包含应用层数据，报文段首部中的标志位SYN置1，简称为SYN报文段。同时客户端随机选取一个初始序号client\_isn，放置于SYN报文段的序号字段中，最后把该报文段经下层封装发送给服务器。客户端发送SYN信号的意思是: 服务器，我想向你发起TCP连接，我的初始序号为client\_isn。
2. 第二步：服务器收到SYN报文段后，响应一个SYNACK报文段。SYNACK报文段的SYN标志位置1，确认号字段设置为client\_isn + 1, 序号字段由服务器选择自己的初始序号server\_isn。SYNACK报文段的意思是：我收到你的SYN报文段，序号为client\_isn，我同意该连接，我的序号为server\_isn。
3. 第三步：客户端接收到SYNACK后告知服务器自己收到了。于是发送最后一个报文段，SYN标志位置0，把确认字段设置为server\_isn +1，并设置自己的序号。这个报文意思是：好的，我知道你同意了，我们开始传输数据吧。

注意：在解释序号和确认号之前先解释一下为什么是三次握手而不是两次握手。

--三次握手



--二次握手

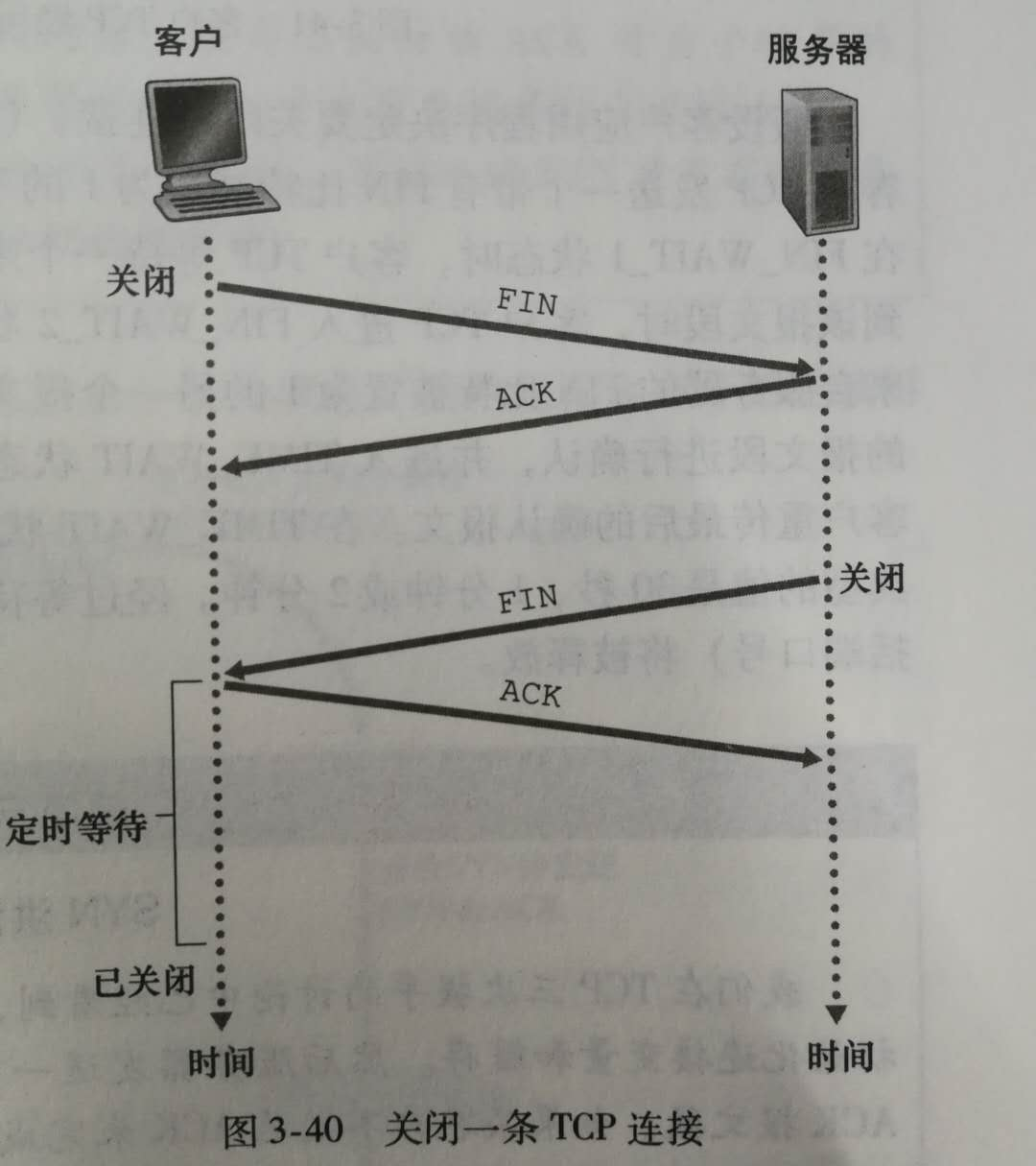


明白了为什么是三次握手而不是二次握手后, 再来看TCP报文段中的序号和确认号.

* 序号:
* 序号是建立在传送的字节流之上, 而不是建立在传送的报文段的序列之上的. 意思是说如果把传输的数据看作是一个字节文本, 序号则是对文本的首字节进行编号.
* 我知道还是很抽象, 看具体例子. 现在要通过TCP发送一个500000字节的大文件, 最大报文长度为1000(一个报文段最多只能装1000个字节). 那么这次TCP传输就要分为500个报文段. 第一个报文段序号为0, 因为在500000字节中首字节的序号为0; 第二个报文段的序号为1000, 因为第一个报文段装了1000个字节, 第二个报文段从第1000个字节开始装起; 同理, 第三个报文段的序号为2000…
* **为什么要使用序号?**
* 发送序号是为了告诉接收方, 下一次我将从哪个地方开始传数据给你. 接收方同时也会期待下次从下一个字节序列的位置开始接收发送方的数据. 接收方会把这个位置写到**确认号**中, 比如上面的例子, 接收方在接收到0序列分组后, 会在确认字段填入1000, 下一次期待接收1000位置的字节.
* 由上可见: 主机A填充进报文段的确认号是主机A期望从主机B收到的下一字节的序号.

TCP四次挥手

--四次挥手指的是TCP的两端断开连接时的四次报文段传输。



1. 首先客户端TCP向服务器发送一个特殊的TCP报文段，其中FIN标志位被置为1
2. 服务器收到该报文段后就向发送方发送一个确认报文段
3. 然后服务器发送自己的终止报文段，同样把FIN位置1
4. 最后客户端对服务器的终止报文端发送确认响应。

## 二、复习题：

## 1、第一章

R1.“主机”和“端系统”之间有什么不同?列举几种不同类型的端系统。Wb服务器是一种端系统吗？

答：（1）没有区别。根据书本内容，“ 主机”和“终端系统”是交换使用。

（2）终端系统：PC、工作站、网络服务器、邮件服务器、PDA（Personal Digital Assistant）、手机、智能手环等连入网的设备都是端系统。

（3）由（2）得，网络服务器是终端设备。

R4. 列出6种接入技术。将他们分类为住宅接入、公司接入或广域无线接入

a)通过电话线的拨号调制解调器：家庭（早就不用了，它采用的是纯电话线上网RJ11）

b)通过电话线的DSL（Digital Subscriber Line，数字用户线）：家庭或小办公室

c)混合光纤（FTTH）同轴电缆:家庭

d)100M交换以太网：企业

e)无线网（wifi）：家庭或者企业

f)3G和4G：广域无线网

补充：调制解调器：用于将数字信号转换为模拟信号传输的，分类有好多，为了更好的发送信号，可以进行调频载波。

a)与b）的区别，首先DSL先采用网线（RJ45）连接到DLS调制解调器然后在连接到电话线（只是借助了双绞线的这个载体）。而拨号全程用的是电话线。这样导致调制方法不同带宽也会有巨大差异。

相同点：都会用到modem，电话线

R5. HFC传输速率在用户间是专用的还是共享的? 在下行HFC信道中, 可能出现碰撞吗? 为什么?

答：HFC（混合光纤同轴电缆网）是用户共享的。在下行HFC信道可能出现碰撞，因为信号是用户共享的，所以有碰撞的可能性。

R8 能够运行以太网的一些物理媒介是什么

在以太网传输的一个比特从一个“发射器”到一个“接收器”直接经过的路段就是一种物理媒介。它包括：双绞铜线、同轴电缆、多模光线缆等。

R10 描述今天最为流行的无线因特网接入技术，对它们进行比较和对照

答：最流行的无线因特网接入技术就是无线局域网IEEE802.11（WIFI）和蜂窝网络（4G）。这里举一个简单的例子：无线设备要和更大的网络连接都要经过基站中继，基站是一个概念，具体到不同的技术上有不同的实现，对于WIFI而言基站是无线局域网的接入点，对于蜂窝网而言基站是蜂窝塔，当我们使用wifi的时候需要在基站几十米的范围内，而使用4G的时候，可以离某个基站几百米甚至一公里。

R12 于分组交换相比，电路交换网络有哪些优点？在电路交换中，TDM比FDM有哪些优点。

答：电路交换网相比于分组交换网的优点是它能预先分配链路的使用，保证某个用户能以固定的速率进行网络传输。

FDM（频分复用）和TDM（时分复用）区别：（有个图没加载出来）

FDM把链路带宽分成固定的大小，每个用户想用链路的部分带宽。

不同于FDM，TDM先把链路在时域上分割为帧，然后在每帧中划出时隙，每个用户在每帧中享有一个时隙，这样不仅做到了为用户分配链路，而且每个用户在属于他的时隙中能享有整个链路的带宽。

R16 考虑从某源主机跨越一条固定路由向某目的主机发送一分组。列出端到端时延中的时延组成成分。这些时延中的哪些是固定的，哪些是变化的？

处理时延：检查分组的首部，决定分组流向何处，检查差错等动作形成处理时延，处理时延是固定的。

排队时延：当一个分组来到路由准备传输前，如果路由器正在传输已经到达的分组，刚到分组就要进行排队等待，这是排队时延的概念，但排队时延是变化的，如果队列为空，路由器会直接对来到的分组进行处理，排队时延为0，内存满了，还会丢包呢。

传输时延：传输时延指分组来到路由器后，路由器把从接收到的分组到把分组推向下一段链路所需要的时间。它是分组长度于链路传输速率的函数，因此传输时延的时间是固定的。

传播时延：指分组从一台路由器传送到另外一台路由器所需要的时间，它由链路的物理媒介决定（光纤、双绞线、电缆等），所以传播时延也是固定的。

R20 假定端系统A要向端系统B发送一个大文件。在一个非常高的层次上，描述端系统怎样从该文件生成文组。当这些分组之一到达某分组交换机时，该交换机使用分组中的什么信息来决定将该分组发到那一条链路上？因特网中的分组交换为什么可以于驱车从一个城市到另一个城市并沿途询问方向类比。

答：

（1）端系统A会以固定的大小把大文件分为多个小的数据块，然后通过协议栈，自顶向下地把数据封装为分组并发送到接收端。

（2）分组交换机接收到分组后，会获取分组首部的一个或多个字段的值，然后到自己的转发表中查询该值该对应转发到那一条链路上。

（3）当我们驾车从一个城市到另一个城市时候，我们只知道目的地，而不知道具体要走的路径，但我们可以通过询问路途中的油站或行人得知下一步的具体路径。分组交换中同样也是只知道源地址和目的地址，途中要经过数个路由器，而路由器会根据目的地告诉分组下一条要走的具体路径。

R23. 因特网协议栈中的5个层次有哪些? 在这些层次中, 每层的主要任务是什么?

（1）应用层: 应用层协议用于各个端系统中的应用程序交换信息分组, 该信息分组称为报文.

（2）运输层: 运输层的作用是在应用程序端点之间传送应用层报文段. 在因特网中有TCP和UDP两种运输协议, 任一个都能封装并运输应用层报文, 运输层的分组称为报文段.

（3）网络层: 网络层负责将运输层的报文段和目的地址封装成数据报, 用于下一层的传输.

（4）链路层: 链路层会把网络层的数据报封装成链路层的帧, 并把该帧传递给下一个结点.

（5）物理层: 物理层的任务是将链路层每帧中的一个个比特移动到下一个节点, 具体会落实到不同的物理媒介(双绞铜线, 光纤等).

R24. 什么是应用层报文? 什么是运输层报文段? 什么是网络层数据报? 什么是链路层帧?

（1）应用层报文指的是在端系统的应用程序之间按照某种协议进行信息交换的分组.

（2）运输层报文段指的是通过TCP/UDP等运输层协议对应用层报文进行封装后所形成的分组, 报文段对报文的传输参数进行了一定的设置, 使其具有了某种特性, 比如面向连接, 确保传递等.

（3）网络层数据报是对运输层报文段和目的地址进行封装后产生的分组. 数据报确定了分组的目的地, 使得分组可以通过网络层从发送方传送到接收方.

（4）链路层帧是对网络层数据报的封装, 它添加了下一个节点的具体地址, 使得分组能够传递到下一个节点.

R25. 路由器处理因特网协议栈中的哪些层次? 链路层交换机处理的是哪些层次? 主机处理的是哪些层次.

各层对应: 一、物理层, 二、链路层, 三、网络层, 四、运输层, 五、应用层

路由器处理第一层到第三层

链路层交换机处理第一层和第二层

主机处理所有五层.

R27. 描述如何产生一个僵尸网络, 以及僵尸网络是怎样被用于DDos攻击的.

DDos攻击(Distributed Denial-of-Service, 分布式拒绝服务攻击)

攻击者会通过恶意软件入侵我们的设备, 并且进一步感染其他设备, 当被感染的设备达到一定数量后变形成可供攻击者操控的僵尸网络.

攻击者利用由数以千计的受害主机形成的僵尸网络, 让每台主机向目标猛烈发送流量, 造成目标服务陷入瘫痪, 完成一次DDos攻击.

## 2、第三章

R1. 假定网络层提供了下列服务。在源主机种的网络层接收最大长度1200字节和来自运输层的目的主机地址的报文段。网络层则保证将该报文段交付给位于目的主机的运输层。假定在目的主机上能够运行许多网络应用进程。

1. 设计可能最简单的运输层协议，该协议将使应用程序数据到达位于目的主机的所希望的进程。假设在目的主机种的操作系统已经为每个运行的应用程序分配了一个4字节的端口号。
2. 修改这个协议，使它向目的进程提供一个“返回地址”。
3. 在你的协议 种，该运输层在计算机网络的核心种“必须做任何事”吗

答：

1. 将此协议称为简单传输协议(STP)。在发送方，STP从发送进程发送不超过1192字节的报文和4字节的头（包含目标端口号）。然后，在网络层加入目标地址保证可以传输数据（发送指令），但无法接收数据。网络层将报文传送到目标主机上的STP。目标主机基于STP检查段中的端口号，从段中提取数据，并将数据传递给由端口号标识的进程。
2. 段现在需要两个头字段用于全双工：源端口字段和目标端口字段。在发送方，STP接受不超过1192字节的数据块。在网络层加4字节的段头包含目标主机地址、源主机地址。总之，STP向每个数据块添加一个8字节的头，分别将目标进程的端口号、源进程的端口号、目标主机地址、源主机地址，放在头中。目的主机收到数据后，根据目的端口号将提取出的数据和源端口号交给指定进程。然后可以把数据返回给源主机。
3. 不需要

R4. 描述应用程序开发者为什么可能选择在UDP上运行应用程序而不是在TCP上运行的原因。

答：

UDP[的优点：

1. 某些流视频程序不希望数据传输时受到拥塞控制。
2. 某些程序不希望通过繁杂的握手环节降低了指令的实时性与执行速度。
3. 某些程序不需要提供可靠传输。

通常，IP电话、IP视频会议应用程序的设计者选择在UDP上运行他们的应用程序。

R5. 在今天的因特网中，为什么语音和图像流量常常是经过TCP而不是UDP发送。（提示：我们寻找的答案与TCP的拥塞控制机制没有关系。）

答：

1. 由于大多数防火墙被配置为阻止UDP通信，因此使用TCP处理视频和语音通信可以让通信通过防火墙。
2. 为了确保数据的完整性, 分组丢失可能会对语音和图像质量产生影响.

R6、当应用程序运行在UDP上时，该应用程序可能得到可靠传输吗？如果能，如何实现。

答：好多层都可以施行可靠传输呀，例如将可靠传输放在应用层协议中。然而，这将需要大量的工作和调试。（例如应用层的请求隔两秒没收到，手动重发）

 比如谷歌的Chrome浏览器中所使用的QUIC协议在UDP之上的应用层协议中实现了可靠性。

R7、假定在主机C上的一个进程有一个具有端口号6789的UDP套接字。假定主机A和主机B都用目的端口号6789向主机C发送一个UDP报文段。者两台主机的这些报文段在主机C都被描述为相同的套接字吗？如果时这样的话，在主机C的该进程将怎样知道源于两台不同主机的这两个报文段。

答：对呀，这两个段将被定向到相同的套接字。由于UDP报文结构中没有IP地址字段，对于每个接收到的段，在套接字接口处，因为在传输UDP包的时候，网络层会附带上源和目的的IP地址的，操作系统将向进程提供IP地址，以确定各个段的起源。

补充：毕竟主机A和B在选端口的时候不知道彼此具体会选什么, 肯定会有选用一样端口号的情况, 主机IP能把它们区分开.

R8、假定在主机C端口80上运行一个web服务器，假定这个Web服务器使用持续连接, 并且正在接收来自两台不同主机A和B的请求. 被发送的所有请求都通过位于主机C的相同套接字吗? 如果它们通过不同的套接字传递, 这两个套接字都具有端口80吗? 讨论和解释之.

答：A和B的请求会通过80端口找到服务器进程，就这里而言它们通过相同的套接字与C相连，这个套接字具有80端口。当它们与服务器进程建立连接的时候，服务器进程会单独为它们分配套接字，通过专门的套接字响应客户端的请求。这两个套接字就不具有80端口了。

R14、假设主机A通过一条TCP连接向主机B发送一个序号为38的4个字节的报文段。在这个相同的报文段中，确认号必定是42

答：错误，概念性错误，确认号是期待接收方想要的序号。

R18 是非判断题。考虑TCP的拥塞控制。当发送方定时器超时时，其ssthresh值将被设置为原来的一半。

答：错误，当发送方定时器超时时，TCP发送方将cwnd设置为1并重新开始慢启动过程，它还将第二个状态变量的值ssthresh设置为cwnd/2，即当检测到拥塞时将ssthresh置为拥塞窗口值的一半。

## 第四章网络层:数据平面