一点废话：

这篇文档是我在金山/有道机翻的基础上根据自己的理解渣翻的，图片是截取官方原答案中的图片，然后在中文中括号内的内容（即【】）是我自己补充的一些知识点或者解释，原意是希望自己以后翻答案时能够看懂，所以有一些自言自语碎碎念的地方希望能够包含，所有的中文小括号都是原文档中就有的官方注释，这两点不要弄混了，我的言语可能有错误的地方，官方的语言除非题目对不上否则都是相当准确的（印象中好像有一道题官方的文档我认为出错了，我会在中括号中指出）。

之所以只有原书习题的部分答案，是因为在找资源的过程中已经有大牛学长给我划了这些重点题，没出现在这篇整理中的题不代表不重要，只是说这些题比较有代表性或启发性，如果希望找到其他题的答案，可以去翻翻官方给的原答案或者看看其他人有没有发过吧。

本人也是考研学子，深知找资源不易，而且答案也有很多不足的地方，至于资源保护，如果有人盗去了就盗去了吧，希望能够帮到一些人就足够了，如果您真的觉得文档有用甚至想打赏，那我也欣然接受您的好意（左支右微），毕竟谁不想赚一点生活费呢，哈哈。

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。web 服务器是一种端系统吗

答：没有区别。端系统包括 PC，工作站，Web 服务器，邮件服务器，PDA，互联网连接的游戏机等。（在本书中，“主机”和“终端系统”是交替使用的。）

R3.标准对于协议为什么重要？

答：标准对于协议很重要，这样人们就可以创建互连的网络系统和产品。

R4.列出六种接入技术，将他们分类为住宅接入、公司接入或广域无线接入。

答：1. 调制解调器电话线拨号：家庭；2. 电话：家庭或小型办公室；3. HFC：家庭；4. 100Mbps 交换以太网：企业；5. wifi（802.11）：家庭或企业：6. 3G 和 4G：广域无线。

R8.能够运行以太网的物理媒体是什么？

答：今天，以太网最常见的运行在双绞线铜线上。它也可以运行在光纤链路上。

R11.（P46）

答：在 t0 时发送主机开始发送。 在时间 T1=L/R1 时，发送主机完成传输，整个数据包在路由器接收（没有传播延迟）。 因为路由器在 t1 时刻有整个数据包，所以它可以在 t1 时刻开始向接收主机发送数据包。 时间 t2=t1 + L/R2，路由器完成传输，整个数据包在接收主机接收（同样，没有传播延迟）。 因此，端到端延迟为 L/R1 + L/R2。【时延的类型：处理、排队、传输、传播】

R12.与分组交换网络相比，电路交换网络有哪些优点？在电路交换网络中，TDM 比 FDM 有哪些优点？

答：一个电路交换网络可以保证一定数量的端到端带宽的持续时间。 今天大多数分组交换网络（包括互联网）不能对带宽做出任何端到端的保证。 FDM 需要复杂的模拟硬件将信号转换成适当的频带。

R13.（P46）

答： a. 可以支持 2 个用户，因为每个用户需要一半的链路带宽

b. 由于每个用户在传输时需要 1Mbps，如果两个或更少的用户同时传输，则最多需要 2Mbps。 由于共享链路的可用带宽为 2Mbps，因此链路前不会出现排队延迟。 然而，如果三个用户同时传输，所需的带宽将是 3Mbps，超过共享链路的可用带宽。 在这种情况下，链接之前会有排队延迟。

c. 给定用户发送的概率=0.2

d. 三个用户同时传输的概率=$C_3^3 p^3 (1-p)^{3-3}$ = $(0.2)^3$=0.008。 由于队列在所有用户发送时增长，队列增长的时间比率（这等于所有三个用户同时发送的概率）为 0.008。

R14.为什么等级结构中级别相同的两个 ISP 通常互相对等？某 IXP 是如何挣钱的

答：如果两个 ISP 不相互对等，那么当他们发送流量给对方时，他们必须通过提供商 ISP’发送流量，他们必须支付运输流量的费用。 通过直接相互观察，这两个 ISP 可以减少他们对供应商 ISP’的付款。 互联网交换点(IXP)（通常是在一个独立的建筑物中，有自己的交换机）是一个会议点，多个 ISP 可以连接和/或对等在一起。 ISP’通过向连接 IXP 的每个 ISP 收取相对较小的费用来赚取利润，这可能取决于发送到 IXP 或从 IXP 接收的流量。【ISP 即互联网服务提供商，而 ISP’可以理解为中介】

R16.考虑从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，这些时延中那些是固定的哪些是变化的？
答：延迟组件是处理延迟、传输延迟、传播延迟和排队延迟。排队延迟是可变的，除了排队延迟之外，其他延迟都是固定的。

R18.【P46】
答：10msec; d/s; no; no（只算传播时延，没有谈及端点发送这个分组）

R19.【P46】
答：a) 500 kbps（吞吐量指发送设备单位时间内发送数据量的多少）
b) 64 seconds
c) 100kbps; 320 seconds

R22.列出一个层次能够执行的 5 个任务，这些任务中的一个（或两个）可能由两个（或更多）层次执行吗？
答：五个通用任务是差错控制、流量控制、分割重组、复用、连接设置。 是的，这些任务可以在不同的层中复制。 例如，差错控制通常提供在多个层。

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？
答：互联网协议栈中的五个层是（从上到下）应用层、传输层、网络层、链路层和物理层。 第 1.5.1 节概述了主要责任。

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（包）？什么是链路层帧？
答：应用层消息：应用程序希望发送并传递到传输层的数据；传输层段：由传输层生成，用传输层报头封装应用层消息；网络层数据报：用网络层报头封装传输层段；链路层帧：用链路层帧头帧尾封装网络层数据报。

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？
答：路由器处理网络、链路和物理层（第 1 至 3 层）。(这有点言过其实，因为现代路由器有时充当防火墙或缓存组件，处理传输层也是如此。）链路层切换进程链路和物理层（层 1 至 2）。主机处理所有五层。

R26.病毒和蠕虫有什么不同？
答：a)病毒需要某种形式的人类互动来传播。 典型例子：电子邮件病毒。
b)蠕虫不需用户复制。感染主机中的蠕虫扫描 IP 地址和端口号，寻找易受感染的进程。

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
答：创建僵尸网络需要攻击者在某些应用程序或系统中找到漏洞(例如。 利用应用程序中可能存在的缓冲区溢出漏洞)。 找到漏洞后，攻击者需要扫描哪些主机是脆弱的。 目标基本上是通过利用这种特定的脆弱性来破坏一系列系统。任何属于僵尸网络的系统都可以通过利用漏洞自动扫描其环境并传播。 这种僵尸网络的一个重要特性是，僵尸网络的发起者可以远程控制和向僵尸网络中的所有节点发出命令。 因此，攻击者可以向所有节点发出命令，即针对单个节点(例如，僵尸网络中的所有节点都可能被攻击者命令向目标发送 TCP SYN 消息，这可能导致对目标的 TCP SYN 洪泛攻击)。

P2.【P47】
答：在 N*(L/R)时，第一个数据包已到达目的地，第二个数据包存储在最后一个路由器中，第三

个数据包存储在下一个路由器中，等等。 当 N*(L/R)+L/R，第二个数据包已到达目的地，第三个数据包存储在最后一个路由器中等。 继续这种逻辑，我们看到当 N*(L/R) + (P-1)*(L/R) = (N+P-1)*(L/R) 所有数据包都已到达目的地。【注意这些全都是存储转发的形式】

P5.【P48】

答：收费亭相距 75 公里，汽车以每小时 100 公里的速度行驶。 收费亭每 12 秒为一辆车服务。

a)有十辆车。 第一个收费站为这 10 辆车服务需要 120 秒，即 2 分钟。 在到达第二个收费站之前，每辆车的传播延迟为 45 分钟(行程 75 公里。 因此，所有的汽车都排在第二个收费站之前，47 分钟后。 整个过程在第二个和第三个收费站之间重复进行。 第三个收费站也需要 2 分钟的时间为这 10 辆车服务。 因此，总延迟为 96 分钟。【题目应是认为“整个车队均通过一个收费站后再一起发车，而不是某辆车通过收费站后不停留立刻发车”，即第一辆车等最后一辆车检查完再发车，而不是最后一辆车还在检查时，前面的 9 辆车已经在路上了，这不符合分组转发的逻辑但题目就是这么问的）

b)收费亭之间的延误为 8*12 秒加 45 分钟，即 46 分 36 秒。 总延迟是这个数量的两倍，加上 8*12 秒，即 94 分 48 秒。

P6.【P48】

答：

a. $d_{prop} = m/s$ seconds.

b. $d_{trans} = L/R$ seconds.

c. $d_{end-to-end} = (m/s + L/R)$ seconds.

d. 该位刚刚离开主机 A

e. 第一位在链接中，尚未到达主机 B

f. 第一位已到达主机 B

g. $m = \frac{L}{R}s = \frac{120}{56\times10^3}\left(2.5\times10^8\right) = 536\,\text{km}.$

P8.【P48】

答：

a.可支持 20 名用户

b. $p = 0.1$.

c. $\binom{120}{n}p^n(1-p)^{120-n}$.

d. $1-\sum_{n=0}^{20}\binom{120}{n}p^n(1-p)^{120-n}$.

我们用中心极限定理来近似这个概率。设 X_j 是独立的随机变量，这样

$$P(\text{“21 or more users”}) = 1 - P\left(\sum_{j=1}^{120} X_j \le 21\right)$$

$$P\left(\sum_{j=1}^{120} X_j \le 21\right) = P\left(\frac{\sum_{j=1}^{120} X_j - 12}{\sqrt{120\cdot0.1\cdot0.9}} \le \frac{9}{\sqrt{120\cdot0.1\cdot0.9}}\right)$$

$$\approx P\left(Z \le \frac{9}{3.286}\right) = P(Z \le 2.74)$$

$$= 0.997$$

【电路交换需要为用户预留一部分带宽，比如题中的 150kbps，不管用户是否活跃这部分带宽始终被某用户占用，因此这也就形成了端到端之间的连接，只要某用户活跃就能通过链路发送消息，而分组交换只在用户需要时才把他的消息放到链路上】

P10.【P48】

答：第一端系统要求 L/R_1 将数据包传输到第一链路上；数据包在 d_1/s_1 中的第一链路上传播；数

据包交换机增加了 d_{proc} 的处理延迟；在接收到整个数据包后，连接第一和第二链路的数据包交换机要求 L/R_2 将数据包传输到第二链路上；数据包在 d_2/s_2 中的第二链路上传播。 同样，我们可以找到由第二个开关和第三个链接：L/R_3、d_{proc} 和 d_3/s_3 引起的延迟。 加上这五个延迟就可以了

$$d_{end\text{-}end} = L/R_1 + L/R_2 + L/R_3 + d_1/s_1 + d_2/s_2 + d_3/s_3 + d_{proc} + d_{proc}$$

为了回答第二个问题，我们简单将值插入方程中，得到 6 + 6 + 6 + 20+16 + 4 + 3 + 3 = 64 毫秒。

P31.【P50】

答: a.从源主机发送消息到第一分组交换机的时间=$\frac{8\times10^6}{2\times10^6} = 4\text{sec}$。与存储和转发交换，将消息从源主机移动到目标主机的总时间=$4\text{sec} \times 3\text{hops} = 12\text{sec}$。

b.从源主机发送第一个数据包到第一个数据包交换机的时间=$\frac{1\times10^4}{2\times10^6} = 5m\ \text{sec}$。在第一交换机接收第二分组的时间=在第二交换机接收第一分组的时间=$2 \times 5\text{m sec} = 10\ \text{m sec}$。【题目说的是从第一个分组开始发送时计时到题设描述的事件发生停止计时之间的时间，不是从一个结点开始发送计时】

c. 在目标主机接收第一个数据包的时间=$5\text{m sec} \times 3\text{hops} = 15\ \text{m sec}$在此之后，每 5msec 将接收一个数据包；因此，在接收最后（800）数据包的时间=$15\text{m sec} + 799 * 5m\ sec = 4.01\ \text{sec}$。可以看出，使用消息分割的延迟明显减少（几乎三分之一）。

d.数据报分段的优点（除了减小时延外）

i. 没有消息分割，如果比特错误是不能容忍的，如果有单个比特错误，则必须重新传输整个消息（而不是单个数据包）。

ii. 在没有消息分割的情况下，巨大的数据包（例如包含高清视频）被发送到网络中。 路由器必须容纳这些巨大的数据包。 较小的数据包必须在巨大的数据包后面排队，并遭受不公平的延迟。

e.数据报分段的缺点

i.数据包必须按顺序放置在目的地。

ii.消息分割导致许多较小的数据包。 由于首部大小通常对所有数据包相同，而不管它们的大小如何，通过消息分割，首部字节的总数更多。

第二章

R1.列出 5 种非专用的因特网应用以及它们所使用的应用层协议。

答：网络：HTTP；文件传输：FTP；远程登录：Telnet；电子邮件：SMTP；比特流文件共享：BitTorrent 协议

R2.网络体系结构与应用程序体系结构之间有什么区别?

答：网络体系结构是指将通信过程组织成层（例如，五层互联网体系结构）。 另一方面，应用程序体系结构由应用程序开发人员设计，并广泛规定应用程序的结构(例如客户机-服务器或 P2P)

R3.对两进程之间的通信会话而言，哪一个是客户？哪一个是服务器?

答：发起通信的进程是客户端；等待联系的进程是服务器。

R5.运行在一台主机上的一个进程，使用什么信息来表示运行在另一台主机上的进程?

答：目的主机的 IP 地址和目的进程中套接字的端口号。

R6.假定你想尽快地处理从远程客户到服务器的事务，你想用 UDP 还是 TCP？为什么。

答：你会用 UDP。 用 UDP，事务可以在一次往返时间(RTT)内完成——客户端将事务请求发送到 UDP 套接字中，服务器将回复发送回客户端的 UDP 套接字。 对于 TCP，至少需要两个 RTT-一个用于设置 TCP 连接，另一个用于客户端发送请求，以及服务器发送回应答。

R10.握手协议的作用是什么?

答：如果两个通信实体在相互发送数据之前首先交换控制数据包，则协议使用握手。 SMTP 在应用层使用握手，而 HTTP 不使用握手。

R11.为什么 HTTP、SMTP、POP3 都运行在 TCP 上，而不是 UDP 上?

答：与这些协议相关的应用程序要求以正确的顺序接收所有应用程序数据，并且不存在间隔。TCP 提供此服务，而 UDP 不提供。

R12.考虑一个电子商务网站需要保留每一个客户的购买记录，描述使用 cookie 来完成该功能

答：当用户第一次访问该站点时，服务器创建一个唯一的标识号，在其后端数据库中创建一个条目，并将此标识号返回为 cookie 号。 此 cookie 编号存储在用户主机上，并由浏览器管理。在随后的每次访问（和购买）期间，浏览器将 cookie 号码发送回站点。 因此，站点知道这个用户（更准确地说，这个浏览器）何时访问站点。

R13.描述 WEB 缓存器是如何减少接收被请求对象的时延的，WEB 缓存器将减少一个用户请求的所有对象或只是其中的某些对象的时延吗？为什么?

答：Web 缓存可以使用户“更接近”所需的内容，这是因为用户主机连接的同一个局域网。 Web 缓存可以减少所有对象的延迟，即使是未缓存的对象，因为缓存减少了链接上的流量。【标准答案说的很模糊，个人版本：首先，WEB 缓存器通常在局域网上，即一些离用户主机比较近的地方，可以将 HTTP 请求的一部分返回内容下载到缓存器自身中，当有用户请求该部分内容时就可以将缓存器中的内容返回给用户而不必再去访问目的服务器，如果访问的是未缓存过的内容就向服务器请求内容，而总的来说由于收束了多个用户的请求为向服务器的一次请求，总是能减少网络上的流量】

R18.从用户的角度来看，POP3 中下载并删除模式和下载并保留模式有什么区别吗?

答：下载并删除模式中，用户从 POP 服务器检索其消息后，消息将被删除。 这给访客用户带

来了一个问题，他们将无法在不同的机器(办公 PC、家庭 PC 等)上访问消息。 在下载并保留模式中，用户检索消息后不会删除消息。 这也可能不方便，因为每次用户把存储的消息转存到新设备时，所有未删除的消息都将被转移到新设备（包括非常旧的消息）。

R21.在 BitTorrent 中，假定 Alice 向 Bob 提供一个 30 秒间隔的文件块吞吐量。Bob 必须进行回报，在相同的间隔中向 Alice 提供文件块吗？为什么。
答：Bob 也不需要向 Alice 提供块。 Alice 必须在 Bob 的前 4 个邻居中，Bob 才能向她发送块；即使 Alice 在 30 秒的间隔内向 Bob 提供块，这也可能不会发生。【BitTorrent 是极其复杂的协议，书中只说了核心思想，就是一个用户需要不断发送并可能会被随机发送数据，与自己产生流量最高的四位则自己可以选择性向对方发送，题目中问的是 Bob 必须给 Alice 发送吗？故答案是不一定，因为 Alice 如果不在 Bob 前 4 位顶流中则 Bob 到 Alice 这条链路是不通的】

R23.覆盖网络是什么？它包括路由器吗？在覆盖网络中边是什么？
答：P2P 文件共享系统中的覆盖网络由参与文件共享系统的节点和节点之间的逻辑链路组成。如果 A 和 B 之间有半永久 TCP 连接，则从节点 A 到节点 B 之间有一个逻辑链路(图论术语中的“边”)。 覆盖网络不包括路由器。

R24.CDN 通常采用两种不同的服务器放置方法，请列举并描述它们。
答：一种服务器放置理念被称为 Enter Deep，它通过在世界各地的访问 ISP 中部署服务器集群，深入到 ISP 的访问网络中。 目标是减少终端用户和 CDN 服务器之间的延迟和提高吞吐量。 另一种理念是 Bring Home，它通过在较少的站点上构建大型 CDN 服务器集群，并将这些服务器集群通常放置在 IXP(Internet Exchange Point)中。 与 Enter Deep 的设计理念相比，Bring Home 的设计通常导致较低的维护和管理成本。

R26.在 2.7 节中描述的 UDP 服务其仅需要一个套接字，而 TCP 服务器需要两个套接字。为什么？如果 TCP 服务器支持 n 个并行链接，每条连接来自不同的客户主机，那么 TCP 服务器将需要多少个套接字？
答：使用 UDP 服务器，没有欢迎套接字，来自不同客户端的所有数据都通过这个套接字进入服务器。 对于 TCP 服务器，有一个欢迎套接字，每次客户端启动到服务器的连接时，都会创建一个新的套接字。 因此，为了支持 n 个同时连接，服务器将需要 n+1 个套接字。

R27.在 2.7 中描述的运行在 TCP 之上的客户-服务器应用程序，服务器程序为什么必须先于客户程序运行？对于运行在 UDP 之上的客户-服务器应用程序，客户程序为什么可以先于服务器程序运行？
答：对于 TCP 应用程序，一旦客户端被执行，它就尝试启动与服务器的 TCP 连接。 如果 TCP 服务器没有运行，那么客户端将无法进行连接。 对于 UDP 应用程序，客户端在执行时不会立即启动连接(或尝试与 UDP 服务器通信)。【TCP 程序一打开就开始向服务器发消息申请建立连接，而 UDP 程序打开后可以先做本地的操作，当然如果不开服务器，UDP 程序发送的消息也是收不到的】

P1.判断题

a.假设用户请求由一些文本和三幅图组成的 Web 页面，对于这个页面，客户将发送一个请求报文并接收四个响应报文。

答：错误。【请求与响应必定成对】

b.两个不同的 Web 页面（如 www.mit.edu/research.html 和 www.mit.edu/students.html）可以通过同一个持续性链接发送。

答：正确。【根路径相同，是一个主机中的不同文件】

c.在浏览器和初始服务器之间使用非持续性链接的话，一个 TCP 报文段是可能携带两个不同的 HTTP 服务请求报文的。

答：错误。

d.在 HTTP 响应报文中的 Date：首部指出了该响应中对象最后一次修改的时间。

答：错误。

e.HTTP 响应报文绝不会具有空的报文体。

答：错误。【HTTP 调用 TCP，必定有确认报文段，如果没有消息回复则无法捎带确认，就会发送一个空内容的报文用于确认】

P3.考虑要获取指定 URL 的 Web 文档的 HTTP 客户，该 HTTP 服务器的 IP 地址未知。在该情况下除了使用 HTTP 外还需要用到什么运输层和应用层协议？

答：应用层：HTTP、DNS；运输层：TCP（为了运行 HTTP）、UDP（为了运行 DNS）。

P8.【P115】

答：首先第 7 题的答案是 $2RTT_0+RTT_1+\ldots+RTT_n$【因为一个 RTT 就是一个往返的时延，因此访问 DNS 的时延是 1~n 各 1 个，接着 HTTP 采取 TCP 连接，需要在第一个 RTT 内建立连接，第二个 RTT 内发送请求并接收应答，故有两个 RTT_0】

a. $18RTT_0+RTT_1+\ldots+RTT_n$【其他部分与第七题一样，然后客户发送一个 HTTP 请求，得到基本 HTML 文件后，经过解析这个 HTML 文件得到 8 个图像的地址，再继续同样的 HTTP 请求 8 次，即在第七题基础上多了 8 个图像的建立连接、请求响应，注意非持续性连接在发送响应后，TCP 连接就立刻断开了，需要继续发送则需要重新申请建立连接】

b. $6RTT_0+RTT_1+\ldots+RTT_n$【客户仍需先请求建立 TCP 连接、发送数据请求并接受 HTML 基本文件，消耗 2 个 RTT_0，接着解析 HTML 文件后同时申请建立 5 个 TCP 连接，消耗 1 个 RTT_0，请求并接收 5 个图像，消耗 1 个 RTT_0，还余下 3 个 RTT_0 仍需申请建立 3 个 TCP 连接、请求并接收 3 个图像】

c.（无并行）$10RTT_0+RTT_1+\ldots+RTT_n$【持续性链接即 a 省掉后续 8 次申请 TCP 的 RTT_0】

（5 并行） $3RTT_0+RTT_1+\ldots+RTT_n$

P11.【P116 另第 10 题有较复杂的情况，但不影响第 11 题解答】

答： a)是的，因为 Bob 有更多的连接，他可以获得更大份额的链路带宽。

b)是的，但鲍勃仍然需要执行并行下载，否则他将获得比其他四个用户更少的带宽。

P13.SMTP 中的 MAIL FROM 与该邮件报文自身中的“From：“之间有什么不同？

答：①MAIL FROM——在 SMTP 中，是来自 SMTP 客户端的消息，该消息能识别发送邮件到 SMTP 服务器的发送者身份。②From：——在邮件消息本身不是 SMTP 消息，而是邮件消息正文中的一行。

P28.在一台主机上安装编译 TCPClient 和 UDPClient 的 Python 程序，在另一台主机上安装编译 TCPServer 和 UDPServer 的程序。

a.假设在运行 TCPServer 之前运行 TCPClient，将会发生什么现象？为什么？

答: 如果首先运行 TCPClient, 那么客户端将尝试与不存在的服务器进程进行 TCP 连接。无法进行 TCP 连接。

b.假设在运行 UDPServer 之前运行 UDPClient，将会发生什么现象？为什么？

答：UDPClient 没有与服务器建立 TCP 连接。 因此，如果首先运行 UDPClient，然后运行 UDPServer，然后在键盘上键入一些输入，那么一切都会正常工作。

c.如果你对客户端和服务器使用了不同的端口，将会发生什么现象？

答：如果使用不同的端口号，那么客户端将尝试与错误的进程或不存在的进程建立 TCP 连接。 将会发生错误。

P30.你能配置浏览器以打开对某 Web 站点的多个并行链接吗？有大量的并行 TCP 连接的优点和缺点是什么？

答：是的，可以配置许多浏览器来打开到 Web 站点的多个同时连接。 优点是可能会更快地下载该文件。 缺点是可能会占用带宽，从而大大减缓共享相同物理链接的其他用户的下载速度。

第三章

R3.假设 A 到 B 的 TCP 报文段具有源端口号 X 和目的端口号 Y，则对于从 B 到 A 的报文段源端口号和目的端口号分别是多少？

答：源端口号 Y 和目的端口号 X。

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：应用程序开发人员可能不希望其应用程序使用 TCP 的拥塞控制，拥塞控制会在拥塞发生时抑制应用程序的发送速率。 通常，IP 电话和 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，因为他们希望避免 TCP 的拥塞控制。 此外，一些应用程序不需要 TCP 提供的可靠数据传输。【如果视频会议采用拥塞控制，则网络拥堵时接收方会看到停止的页面，然后在网络恢复后会看到视频中的对象以极快速度完成一系列播放直到跟上当前时间点，若落后过多则需要消耗大量时间播放一系列无意义的内容，导致观众丢失更多内容，如果用 UDP 则网络恢复后会直接从当前时间点开始进行】

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：与拥塞控制无关。

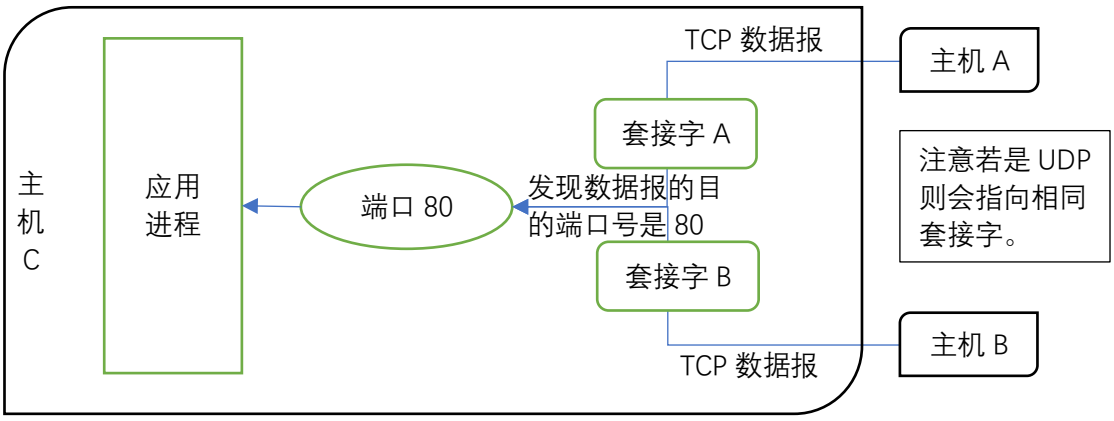
答：由于大多数防火墙被配置为阻止 UDP 通信，因此使用 TCP 进行视频和语音通信可以通过防火墙进行通信。

R7.若主机 C 上有一个进程具有端口号 6789 的 UDP 套接字。假定主机 A 和主机 B 都用目的端口号 6789 对主机 C 发送一个 UDP 报文段。这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？如果这样的话，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：是的，两个报文段都将指向同一个套接字。 对于每个接收到的报文段，在套接字接口处，操作系统将向进程提供 IP 地址，以确定单个报文段的源主机。

R8.若主机 C 端口 80 上运行一个 Web 服务器，假设这个 Web 服务器使用持续链接，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？如果他们通过不同的套接字传递，这两个套接字都具有端口 80 吗？

答：对于每个持续连接，Web 服务器创建一个单独的“连接套接字”。 每个连接套接字用四个元组标识：(源 IP 地址，源端口号，目的 IP 地址，目的端口号)。 当主机 C 接收 IP 数据报时，它检查数据报/段中的这四个字段，以确定它应该将 TCP 段的有效负载传递给哪个套接字。因此，来自 A 和 B 的请求通过不同的套接字。 这两个套接字的目的端口都是 80；但是，这些套接字有不同的源 IP 地址。 与 UDP 不同，当传输层将 TCP 段的有效负载传递给应用程序进程时，它不指定源 IP 地址，因为这是由套接字标识隐式指定的。【如下图】



R9.在我们的 rdt 协议中，为什么需要引入序号？
答：接收主机需要序列号来确定到达的数据报是否包含新数据或重新传输。

R10.在我们的 rdt 协议中，为什么需要引入定时器？
答：用来处理传输链路上的丢失情况。 如果在该分组的定时器持续时间内没有接收到传输分组的 ACK，则假定该分组(或 ACK 又或 NACK)已丢失。 于是，数据包被重传。【rdt 总结】

rdt1.0：只考虑信道理想，不存在差错，发送方只管发、接收方只管收。
rdt2.0：信道可能出现差错但不会丢包，因此发送方**引入等待机制**，发完消息后等接收方送一个 ACK（接收方已成功收到）或 NAK（也写作 NACK，表示接收方发现分组有误需要重传），发送方收到 ACK 则发下一个分组，收到 NAK 则退回之前的状态，发送有问题的分组。注意 NAK 是表示接收方经过校验和之类手段发现分组有问题时由接收方发送的，而不是超时信号。由于 rdt2.0 发送方只有两个状态，这样的协议被称为“停等协议”，但注意 rdt2.0 可能因为 ACK 或 NAK 损坏而导致发送方不清楚接收方意图，因而无论是重发还是发送下一分组都可能导致传输崩溃，因此 rdt2.0 是不可运行的。如接收方已收到分组并发送 ACK，在信道上损坏而导致发送方不可读，若重发则接收方会收到一个重复分组而导致收发两端错乱。
rdt2.1：**引入序号**，分次调用。这样 rdt2.0 的收发两端错乱问题就解决了，接收方可以发现并报告收到了重复分组（因为可以比对序号了，而比对分组内容是否一致是不可行的）。
rdt2.2：不再使用 NAK，一旦发现**收到的分组损坏则报告上一次正确接收序号的确认**。如分组 0 正常收到，分组 1 损坏，则在发现分组 1 损坏后给发送方发送一个 ACK0 而不发送 ACK1。
rdt3.0：在此协议中考虑比特受损的情况和信道丢包的情况，**引入定时器**，发送消息后启动倒计时，超过时间了还未收到 ACK 则认为丢包，直接重传，超时后收到该分组的确认则立刻发送下一分组，同时接收方收到重复的分组则仍发送该分组的确认 ACK，发送方收到以前分组的确认则什么也不做。rdt3.0 有时也称为“比特交替协议”。

R11.假设发送方和接收方之间的往返时延是固定的并且为发送方所知，假设分组能够丢失的话，在协议 rdt3.0 中，一个定时器仍是必须的吗？
答：在协议 rdt3.0 中仍然需要计时器。 如果已知往返时间，那么唯一的优势将是，发送方确信数据包或数据包的 ACK(或 NACK)已经丢失，与实际场景相比，在计时器过期后，ACK(或 NACK)可能仍在发送方的路上。 然而，为了检测每个数据包的丢失，发送方仍然需要计时器。【即仍需要一个计时的功能，知道往返时间也只是时间到了能够确信确认超时而已】

R14.判断题

a.主机 A 经过一条 TCP 连接向主机 B 发送一个大文件。假设主机 B 没有数据发往主机 A，则因为主机 B 不能随数据捎带确认，所以主机 B 将不向主机 A 发送确认。

答：错误。

b.在连接的整个过程中，TCP 的 rwnd 长度决不会变化。

答：错误。

c.假设主机 A 通过一条 TCP 连接向主机 B 发送一个大文件，主机 A 发送但未被确认的字节数不会超过接收缓存的大小。

答：正确。

d.假设主机 A 通过一条 TCP 连接向主机 B 发送一个大文件。如果对于这条链接的一个报文段的序号为 m，则对于后继报文段的序号将必然是 m+1。

答：错误。【这个 m 可能是重传的，重传后回归正常顺序，就不知道是不是 m+1 了】

e.TCP 报文段在它的首部中有一个 rwnd 字段。

答：正确。

f.假定在一条 TCP 连接中最后的 SampleRTT 等于 1 秒，则对于该链接的 TimeoutInterval 的当前值必定大于等于 1 秒。

答：错误。【超时时间的计算与均值 RTT 有关，而均值 RTT 的计算公式中样本 RTT 是有权值的，不是大于等于的关系，具体公式和计算过程 P158、P159】

g.假设主机 A 通过一条 TCP 连接向主机 B 发送一个序号为 38 的四字节报文段。在这个相同的报文段中，确认号必然是 42。

答：错误。

R15.假设主机 A 通过一条 TCP 连接向主机 B 发送两个紧挨着的 TCP 报文段。第一个报文段的序号为 90，第二个报文段序号为 110。

a.第一个报文段中有多少数据？

答：20B。【或 20byte，TCP 是面向字节的】

b.假设第一个报文段丢失而第二个报文段到达主机 B。则 B 发往 A 的确认报文中，确认号应该是多少？

答：90。

R17.假设两条 TCP 连接存在于一个带宽为 Rbps 的瓶颈链路上。它们都要发送一个很大的文件（以相同的方向经过瓶颈链路），并且两者是同时开始发送文件。那么 TCP 将为每条连接分配什么样的传输速率？

答：R/2。【默认分配等权重的带宽】

R18.判断“考虑 TCP 拥塞控制，当发送方定时器超时时，其 ssthresh 值被设置为原来值的一半”。

答：错误。【是设置为当前拥塞窗口 cwnd 值的一半，ssthresh 是阈值或者说门限值】

P2.考虑 P129 图 3-5，从服务器返回客户端进程的报文流中源端口号和目的端口号分别是多少？在承载运输层报文段的网络层数据包中，IP 地址是多少？

答：【即将源目 IP、源目端口均反过来填】

假设主机 A、B 和 C 的 IP 地址分别为 a、b、c。（a、b、c 不同）

到主机 A：源端口=80，源 IP 地址=b，目的端口=26145，目的 IP 地址=a

到主机 C，左进程：源端口=80，源 IP 地址=b，目的端口=7532，目的 IP 地址=c

到主机 C，右进程：源端口=80，源 IP 地址=b，目的端口=26145，目的 IP 地址=c

P3.【P189，计算 UDP 和 TCP 的反码检验和】

答：11010001。【按位相加，超 1 进位，**求和的溢出要加到最后一位上，最后整个数求反码】**

为了检测错误，接收者向报文段添加了四个字节（三个原始字节和校验和）。 如果接收方把四个字节相加，所得的和包含零则接收方认为收到的报文段存在错误。 所有的一位错误都会被检测到，但是两位错误可能不被检测到（如果第一个字的最后一位被转换为 0，第二个字的最后一位被转换为 1）。

P4. a.假定有下列两个字节：01011100 和 01100101。这两个字节和的反码是多少？

答：和为 11000001，反码为 00111110。

b.假定有下列两个字节：11011010 和 01100101。这两个字节和的反码是多少？

答：和为 01000000，反码为 10111111。

c.对 a.中的字节，给出一个例子，使这两个字节中的每一个都在一个比特反转时，其反码不会改变。

答：分别转为 01010100 和 01101101。【即两个字的第 i 位同时反转】

P5.假设某 UDP 接收方对接收到的 UDP 报文段计算因特网检验和，并发现它与承载在检验和字段中的值相匹配，该接收方能够绝对确信没有出现过比特误差吗？解释原因。
答：不，接收方不能绝对确定没有发生位错误。 这是因为计算数据包校验和的方式。 如果数据包中两个 16 位字的相应位（将加在一起）为 0 和 1，那么即使这些位分别翻转到 1 和 0，和仍然保持不变。 因此，接收机计算的 1s 补码也将是相同的。 这意味着即使有传输错误也能通过验证。【即前面提过多次了的，多个字节可能同时发生反转导致检验和不变】

P22.考虑一个 GBN 协议，发送窗口为 4，序号范围是 1024。假设在 t 时刻接收方期待的下一个有序分组的序号是 k。媒体不会对报文重新排序，回答以下问题并解释为什么：

a.在 t 时刻，发送方窗口内的报文序号可能是多少？

答：有一个 N=4 的窗口大小。 假设接收器已经接收到数据包 k-1，并已将该数据包和所有其前面的数据包确认了。 如果所有这些 ACK 都被发件人收到，那么发送窗口是[k，k+N-1]。 接下来假设没有一个 ACK 被发件人收到。 在第二种情况下，发送方的窗口包含 k-1 和 N 个数据包，直到并包括 k-1。 发送者的窗口因此是[k-N，k-1]。 总之，序号开始于范围[k-N，k]的某个地方，发送窗口大小 N 为 4，序号[k-N, k+N-1]都有可能出现在窗口内。

b.在 t 时刻，当前传播给发送方的所有可能报文中，ACK 字段的所有可能值是多少？

答：如果接收器正在等待分组 k，那么它在此之前已经接收了(并确认了)分组 k-1 及其之前的 N-1 个分组。 如果发送方尚未收到这 N 个 ACK，那么值为[k-N，k-1]的 ACK 消息可能仍在向发送方传播。 因为发送方已经发送了数据包[k-N，k-1]，所以发送方必须已经收到了 k-N-1 的 ACK。 一旦接收方为 k-N-1 发送了 ACK，它就永远不会发送小于 k-N-1 的 ACK。 因此，ACK 值的范围是[k-N，k-1]。【原书的答案是“**range from k-N-1 to k-1**”但是如果 ACK(k-N-1)还在链路上传播或刚刚才被发送方接收那么序号为 k-1 的报文是发不出去的，但事实上接收方已成功接收第 k-1 号报文并发送确认了，所以应该 k-N-1 号报文的确认已经到达过发送方才对，不知道是个人理解有误还是答案错了】

P24.判断题，并简要说明原因

a.对于 SR 协议，发送方可能会收到落在其当前窗口之外的分组的 ACK。

答：是的。【总之就是，考虑了超时】 假设发送方的窗口大小为 3，并在 t_0 处发送数据包 1、2、3。 在 t_1（$t_1>t_0$）接收方收到分组并发送 ACK1，2，3，这三个确认报文在链路上超时了。 在 t_2（$t_2>t_1$）发送方发现超时并重新发送 1、2、3。 在 t_3 时，接收方接收副本并重新确认 1、2、3。 在 t_4 时，发送方接收到接收方在 t_1 时发送报文的对应 ACK，并将其窗口提前到 4、5、6。 在 t_5 时，发送方接收 t_2 时发送报文的对应 ACK1、2、3。 这些 ACK 在它的窗口外面。

b.对于 GBN 协议，发送方可能会收到落在其当前窗口之外的分组的 ACK。

答：是的。 理由同 a.。

c.当发送方和接收方窗口长度都为 1 时，比特交替协议与 SR 协议相同。

答：是的。 理由见 d.。

d.当发送方和接收方窗口长度都为 1 时，比特交替协议与 GBN 协议相同。

答：是的。 注意，窗口大小为 1 时，SR、GBN 和交替位协议在功能上是等价的。 窗口大小 1 排除了无序数据包（在窗口内)的可能性。 在这种情况下，累积 ACK 只是一个普通的 ACK，因为它只能引用窗口内的单个数据包。

P26.考虑从主机 A 向主机 B 传输 L 字节的大文件，假设 MSS 为 536 字节。

a.为了使得 TCP 序号不至于用完，L 的最大值是多少？提示 TCP 的序号字段为 4 字节。

答：$2^{32} = 4{,}294{,}967{,}296$。序列号不随每个分组增加，相反它以发送的数据字节数递增【即 TCP 是以字节编号的】。 因此，MSS 的大小是不相关的——可以从 A 发送到 B 的最大大

小文件只是可表示的字节数为2^{32}。

b.对于 a.中的 L，求出传输此文件需要的时间。假定运输层、网络层和数据链路层首部共 66 字节，并加在每个报文段上，经过 155Mbps 链路发送得到的分组。忽略流量控制和拥塞控制，主机 A 能够一个接一个并连续不断地发送报文。

答：分片$\left\lceil \frac{2^{32}}{536} \right\rceil = 8{,}012{,}999$段，将 66 字节的头部添加到每个段中，总共有 528,857,934 字节的头部。 传输的字节总数为$2^{32} + 528{,}857{,}934 = 4.824 \times 10^9$字节。因此，通过 155Mbps 的链路传输文件需要 249 秒。【拥塞窗口 cwnd 的单位是 MSS，即比如在慢启动之初，cwnd 是 1 个窗口，则在第一段时间内发送 536 字节的 TCP 数据字段，在这道题中，MSS 就是指一个分片的数据内容上限，MSS 的值不包含首部长度】

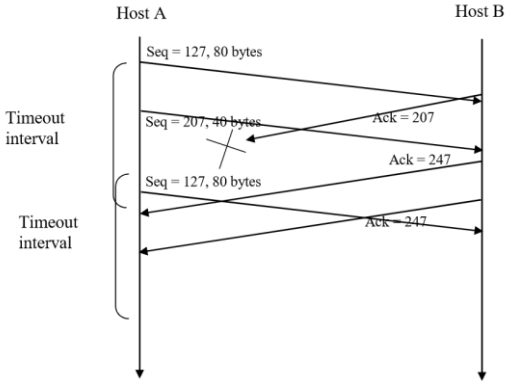
P27.【P192】

答： a.207；302；80

b.207；80；302

c.127

d.



P38.【P193】

答：是的，发送率总是大致为 cwnd/RTT。

P40.【P193，**TCP 拥塞控制的大综合，很重要】**

答： a.答：慢启动间隔为[1, 6]和[23, 26]。【不要漏了某段区间】

b.答：拥塞避免间隔为[6, 16]和[17, 22]。

c.答：3 次重复确认。

d.答：超时。

e.答：32。

f.答：21。【不要看图猜位置，要从头开始 2 4 8 16 的算出点的纵坐标，另外，《自顶向下》和谢希仁版的《计算机网络》解题用的 TCP Reno 版本不一样，《自》在发现三次重复确认后阈值减半，但拥塞窗口减半再加三，《计》在发现三次重复确认后阈值和窗口都仅减半】

g.答：14。【奇数时计算阈值向下取整】

h.答：第 7 轮次。

i.答：4 和 7。【注意三次重复确认时阈值减半，窗口减半加三】

j.答：21；8。【TCP Tahoe 和 TCP Reno 分别是老版本 TCP 和较新版 TCP，Tahoe（老版）无论遇到三次重复确认还是超时重传，处理方式都是阈值减半，窗口归 1，开始慢启动，Reno（新版）引入了快速恢复的协议内容，同时 Reno 也有各种版本，其中两个在 f.中提到了】

k.答：52。【如果慢启动下 cwnd 即将超过 ssthresh，如 cwnd=16，ssthresh=21，则下一轮次 cwnd=21，然后立刻开始拥塞避免】

第四章

R1.网络层的分组名字是什么？路由器与链路层交换机之间的根本区别是什么？

答：网络层的分组就是数据报。 路由器根据数据包的 IP（第 3 层）地址转发数据报。 链路层交换机根据数据包的 MAC（第 2 层）地址转发帧。

R2.我们注意到网络层功能可被大体分成数据平面功能和控制平面功能。数据平面的主要功能是什么？控制平面的主要功能是什么？

答：数据平面的主要功能是数据包转发，即将数据报从其输入链路转发到其输出链路。 例如，数据平面的输入端口执行物理层功能，在路由器上终止传入的物理链路，执行链路层功能与传入链路另一侧的链路层进行互操作，以及在输入端口执行查找功能。 控制平面的主要功能是路由，它是确定数据包从其源到目的地的路径。 控制平面负责执行路由协议，响应向上或向下的附加链路，与远程控制器通信，并执行管理功能。

R3.我们对网络层执行的转发功能和路由选择功能进行区别。路由选择和转发的主要区别是什么？

答：路由和转发之间的关键区别在于，转发是路由器将数据包从其输入接口传输到其输出接口的本地操作，转发发生在非常短的时间内（通常是几纳秒），因此通常在硬件中实现。 路由是指确定数据包从源到目的地的端到端路径的全网络进程。路由发生在更长的时间上（通常是秒），并且通常在软件中实现。

R4.路由器中的转发表主要有什么作用？

答：转发表在路由器中的作用是保存条目，以确定数据报通过路由器的哪个输出接口。

R6.我们常看到路由器由输入端口、输出端口、交换结构和路由选择处理器组成，其中哪些是由硬件组成的，哪些是由软件组成的，为什么？转到网络层的数据平面和控制平面的概念，哪些是用硬件实现的，哪些是用软件实现的，为什么？

答：①输入端口、交换结构和输出端口都是在硬件中实现的，因为需要实现的数据报处理速度对于软件实现来说太快了。 传统路由器内部的路由处理器使用软件执行路由协议，维护路由表和附加链路状态信息，并计算路由器的转发表。 此外，SDN 路由器中的路由处理器还依赖于与遥控器通信的软件，以便接收转发表项并将它们安装在路由器的输入端口中。②数据平面通常是在硬件中实现的，因为需要快速处理，例如在纳秒的时间尺度上。 控制平面通常在软件中实现，并以毫秒或秒为尺度，例如执行路由协议，响应向上或向下的附加链接，与远程控制器通信，并执行管理功能。

R7.为什么在高速路由的每个输入端口都有存储转发表的影子副本？

答：使用影子副本，转发查找在本地进行，在每个输入端口处，而不是调用集中式路由处理器。这种分布式的方法避免了在路由器中的单个点上创建查找时遇到处理瓶颈。

R8.基于目的地转发意味着什么？这与通用转发有什么不同？两种方法中哪种是软件定义网络所采用的？【两种转发的细节区别见复习题 R32，答案以复习题 R8 为准即可】

答：基于目的地的转发意味着到达路由器的数据报将仅基于数据报的最终目的地来转发到输出接口。 通用转发意味着，除了其最终目的地外，当路由器确定数据报的输出接口时，还会考虑与数据报相关的其他因素。 软件定义的网络采用通用转发，例如，除了目标 IP 地址外，转发决策还可以基于数据报的 TCP/UDP 源或目标端口号。

R10.列出三种交换结构，哪一种能够跨越交换结构并行发送多个分组？

答：经内存交换；经总线交换；经互联网络交换。【内存式；总线式；纵横式。P207 三种交换技

术的简单图像要能画出来】 经互联网络交换可以并行转发数据包，但要求所有数据包被转发到不同的输出端口。

R11.描述在输入端口会出现分组丢失的原因。描述在输入端口如何消除分组丢失。
答：如果数据包到达路由器的速率超过交换结构的速率，则数据包需要在输入端口排队。 如果这种速率不匹配持续存在，队列将越来越大，最终溢出输入端口缓冲区，导致丢包。 如果交换结构的速度至少是输入速度的 n 倍，其中 n 是输入端口数，则可以消除分组丢失。

R14.我们学习了 FIFO、优先权、循环（RR）和加权公平排队（WFQ）分组调度规则。这些排队规则中，哪个规则确保所有分组是以到达次序离开的？
答：只有 FIFO 才能确保所有数据包按照它们到达的顺序离开。

R15.举例说明为什么网络操作员要让一类分组的优先权超过另一类分组？
答：例如，承载网络管理信息的数据包应该比常规用户流量优先。 另一个例子是，实时语音转换 IP 数据包可能需要比电子邮件等非实时流量获得优先级。

R16.RR 和 WFQ 分组调度之间的基本差异是什么？存在 RR 和 WFQ 完全相同的场合吗？
答：对于 RR，所有服务类都被平等对待，即没有服务类比任何其他服务类具有优先级。 使用 WFQ，服务类被不同的对待，即每个类可以在任何时间间隔内获得不同数量的服务。 当 WFQ 的所有类具有相同数量的服务权重时，WFQ 与 RR 相同。

R17.若主机 A 向主机 B 发送封装在一个 IP 数据报中的 TCP 报文段，当 B 接收到该数据报时，主机 B 中的网络层怎样知道它应当将该数据报交给 TCP 而不是 UDP 或某个其他东西呢？
答：IP 数据报中的 8 位协议字段包含目标主机应该将段传递给哪个传输层协议的信息。

R18.在 IP 首部中，哪个字段能用来确保一个分组的转发不超过 N 台路由器？
答：生存时间（TTL）。

R20.一个大数据报被分割成多个较小的数据报发生在什么时候？较小的数据报在什么地方装配成大数据报？
答：数据报长度超过被封装的数据长度上限时会被分割。 数据报的组装发生在目的主机。【IPv4 允许在链路上分割，即 IPv4 路由器有权分割，但 IPv6 不允许在链路上分割，超长则丢弃，两者的组装都只能由目的主机完成】

R21.路由器有 IP 地址吗？如果有，有多少个？
答：有，路由器有多少个接口就有多少个 IP 地址。【要为每个接口分配一个】

R22.IP 地址 223.1.3.27 的 32 比特二进制等价形式是什么？
答：11011111.00000001.00000011.00011011。

R24.假设在源主机和目的主机之间有 3 台路由器。不考虑分片，一个从源主机发送给目的主机的 IP 数据报将通过多少个接口？为了将数据报从源移动到目的地，需要检索多少个转发表？
答：8 个接口；3 张转发表。【主机是有转发表的，第二问应只考虑了数据报在链路上的传输】

R25.假设某应用每 20ms 生成一个 40 字节的数据块，每块封装在一个 TCP 报文段中，TCP 报文段再封装在一个 IP 数据报中。每个数据报的开销有多大？应用数据所占百分比是多少？
答：TCP 头部和 IP 头部都是 20 字节【题目均默认最少首部情况，不考虑变长】，因此每个数据

报开销 80 字节。 应用数据所占百分比 50%。

R27.“路由聚合”一词意味着什么？路由器执行路由聚合为什么是有用的？
答：路由聚合意味着 ISP 使用一个前缀来声明多个网络。 路由聚合是有用的，因为 ISP 可以使用这种技术向互联网的其他部分声明 ISP 拥有的多个地址前缀相同的网络。

R28.“即插即用”和“零配置”协议意味着什么？
答：“即插即用”和“零配置”协议意味着该协议能够自动配置设备的网络相关方面，以便将主机连接到网络中而不需要网络管理员人工配置。

R30.比较并对照 IPv4 和 IPv6 首部字段，它们有相同的字段吗？
答：IPv6 有一个固定长度的报头，它不包括 IPv4 报头可以包含的大多数选项。 即使 IPv6 报头包含两个 128 位地址(源和目标 IP 地址)，整个报头的固定长度仅为 40 字节。 某些方面的设计理念是相似的。 流量类型、有效负载长度、IPv6 中的下一个首部和跳数限制分别类似于服务类型、数据报长度、协议字段和 IPv4 的生存时间。

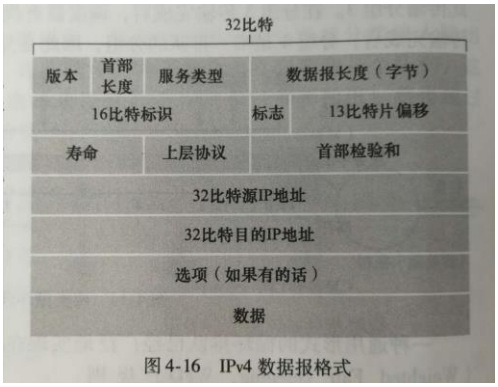


图 4-16 IPv4 数据报格式

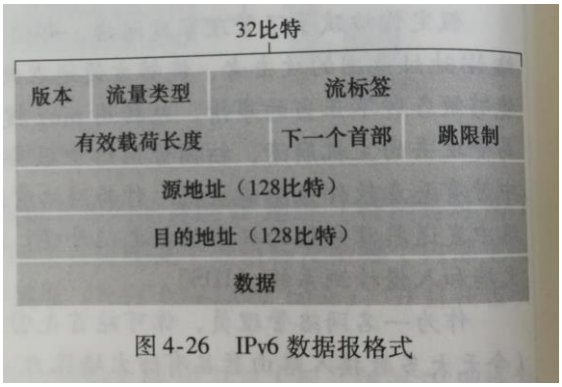


图 4-26 IPv6 数据报格式

【助记：IPv4“版首服总识志移，生协检源目”，“当前版本第一的服务器老总认识志移这个人，是在生鲜协会原来检查比目鱼的”；IPv6“版量流有夏眺原木”，“量版流川枫手办有一个姿势是在夏天眺望森林大树”，要特别记得 IPv6 的源目 IP 是 128 比特，实际上各自占了四行，图中出于简化考虑只画了一行】

R31.有人说当 IPv6 以隧道形式通过 IPv4 路由器时，IPv6 将 IPv4 隧道作为链路层协议，你同意这种说法吗？
答：同意，因为整个 IPv6 数据报包括报头字段，都封装在 IPv4 数据报中。【计算机网络的各层在计算机中并不是泾渭分明的，是为了学习和使用的标准化人为界定的，只要某协议的数据单元将另一协议的数据单元封装进自己的数据部分，就可以认为前者是后者的下一层】

R32.通用转发与基于目的地的转发有何不同？【作为 R8 的补充，就按 R8 来回答也可以】
答：转发有两个主要操作：匹配和执行。 在基于目的地的转发中，路由器的匹配操作只查找待转发数据报的目标 IP 地址，路由器的执行操作涉及将数据包发送到指定的输出端口。 而通用转发，可以在协议栈中不同层与不同协议相关联的多个报头字段上进行匹配，该转发的执行操作可以包括将数据包转发到一个或多个输出端口、跨多个传出接口负载平衡数据包、重写报头值(如 NAT)、故意阻塞/丢弃数据包（如防火墙）、将数据包发送到特殊服务器进行进一步处理和操作等。

P1.【图见 P238】
a.写出路由器 A 中的转发表，使目的地为主机 H3 的所有流量都通过接口 3 转发。

答：　目的地址　　链路接口

H3　　接口 3

b.写出路由器 A 中的转发表，使得从 H1 发往主机 H3 的所有流量都通过接口 3 转发，从 H2 发往主机 H3 的流量通过接口 4 转发。

答: 不可实现, 因为转发规则只基于目的地地址, 无法基于源地址选择转发的链路接口。【即使是通用转发也没有检索数据报源地址的操作】

P2.设两个分组在同一时刻到达同一台路由器的两个不同输入端口，且不考虑其他分组。

a.设这两个分组朝不同的输出端口转发，当交换结构使用一条共享总线时，两个分组可能在相同时可通过该交换结构转发吗?

答：不能，只能在共享总线上一次传输一个数据包。

b. 设这两个分组朝不同的输出端口转发，当交换结构使用经内存交换时，两个分组可能在相同时可通过该交换结构转发吗?

答：不能，正如本书所讨论的，在共享系统总线上一次只能完成一个内存读/写。

c. 设这两个分组朝相同的输出端口转发，当交换结构使用纵横式时，两个分组可能在相同时间通过该交换结构转发吗?

答: 不能, 在此情况下, 两个数据包必须同时通过相同的输出线路发送, 这是不可能的。

P5.【转发表见 P238】

a.提供一个具有五个表项的转发表，使用最长前缀匹配，转发分组到正确的链路接口。

答：

前缀匹配	接口
11100000 00	0
11100000 01000000	1
1110000	2
11100001 1	3
其他	3

【要求是 5 个表项所以必须要拆一个，但接口 2 是没必要拆的，从“其他”中取一个范围外的前缀即可】

b.描述你的转发表是如何为具有下列目的地址的数据报决定适当的链路接口的。

11001000 10010001 01010001 01010101

11100001 01000000 11000011 00111100

11100001 10000000 00010001 01110111

答：第一个地址的前缀匹配是第 5 个条目：链路接口 3；第二个地址的前缀匹配是第三个条目：链路接口 2；第三个地址的前缀匹配是第四个条目：链路接口 3。

P6.【P239】

答：

Destination Address Range	Link Interface
00000000 through 00111111	0
01000000 through 01011111	1
01100000 through 01111111	2
10000000 through 10111111	2
11000000 through 11111111	3

【注意“其他”要找出余下的地址】

0、1、2、3 号接口地址数量分别是：64；32；96；64

P7.【P239】

答：

Destination Address Range	Link Interface
11000000 through (32 addresses) 11011111	0
10000000 through(64 addresses) 10111111	1
11100000 through (32 addresses) 11111111	2
00000000 through (128 addresses) 01111111	3

【写最长前缀匹配转发表的方法是，从最高位 0 开始写，看属于哪个接口，本题中 128 可以直接判断出经过 3 接口转发，然后从 1 开始写，接着第二位是 0 的，又可以写完 64 个地址，然后依然是第一位 1，但第二位是 1，发现可以把接口 2 的 32 位写完，如此递归，最后检查有没有遗漏的前缀，都要往接口 3 转发，本题中正好没有遗漏】

P8.【P239】

答：223.1.17.0/26；223.1.17.128/25；223.1.17.192/28。【子网 3 只要满足子网号 28，且不与另两个子网有交集即可】

P11.考虑一个具有前缀 128.119.40.128/26 的子网。给出能被分配给该网络的一个 IP 地址（形式为 xxx.xxx.xxx.xxx）例子。假设一个 ISP 拥有形式 128.119.40.64/26 的地址块，他要从该地址块中生成 4 个子网，每块具有相同数量的 IP 地址，这 4 个子网的前缀是什么？（形式为 a.b.c.d/x）

答：范围从 128.119.40.128/26 到 128.119.40.191/26 均可。【无分类编址下可以取主机号全零全一，但一般不这么用，习惯上答题是不取全零全一的因为这样稳对，出题老师一般不会在无分类编址的全零全一上设置考点，一般是在子网掩码下考察不可全零全一，全零子网地址，全一广播地址】。4 个子网前缀分别是 128.119.40.64/28，128.119.40.80/28，128.119.40.96/28，128.119.40.112/28。

P14.考虑向具有 700 字节 MTU 的一条链路发送一个 2400 字节的数据报。假定初始数据包标有标识号 422。将会生成多少个分片？在生成相关分片的数据包中各个字段的值是多少？
答：由于 IP 数据报首部有 20B 开销，这个 2400B 的数据报含有 2380B 有效数据，每个分片携带 680B 有效数据，因此分片数为 4。 每个片段将有识别号 422【标识号用于标明哪些片段是属于一个数据报的】。 除最后一个片段外，每个片段的大小为 700 字节(包括 IP 头)。 最后一个数据报的大小为 360 字节(包括 IP 头)。 这 4 个片段的偏移量将为 0、85、170、255【偏移量单位为 8B】。 前 3 个片段中的每个片段将有标志=1；最后一个片段将有标志=0。【答题时写成谢希仁《计算机网络》上的答题表格格式最佳】

P15.若源主机 A 和目的主机 B 之间的数据报被限制为 1500 字节（含 20B 首部）。要发送一个 5MB 的 MP3 文件需要多少个数据报？解释计算过程。
答：MP3 文件大小=500 万字节。 假设数据是在 TCP 段中携带的，**每个 TCP 段也有 20 个字节的首部**。 然后**每个数据报可以携带 1500-40=1460 字节**的 MP3 文件，那么需要数据报的数量为 $\left\lceil \frac{5\times10^6}{1460} \right\rceil = 3425$。除了最后一个数据报之外，所有的都是 1500 字节；最后一个数据报将是 960+40=1000 字节。 请注意，这里没有碎片——源主机不创建大于 1500 字节的数据报，并且这些数据报小于链接的 MTU。【注意计算时应用层数据是传输层的有效载荷，传输层的数据被分片时需要重新添加 TCP 头部，所以计算时要考虑 40B 头部，这种题的识别要点是题目给的是应用层数据长度，而不是网络层发下来的数据包长度，一些学校的期末题也考了，而且都是按照 TCP 算的，没有考虑 UDP】

第五章

R4.比较和对照链路状态和距离矢量这两种路由选择算法。

答：链路状态算法：使用关于网络的完整的全局知识计算源和目的地之间的最小成本路径。 距离矢量路由：以迭代、分布式的方式计算最小成本路径。节点只知道它应该转发数据包的邻居，以便沿着最小成本的路径到达给定的目的地，以及该路径从自己到目的地的成本。

R5.在距离矢量路由选择中的“无穷计数”是什么意思？

答：“无穷计数”问题是指距离矢量路由问题。 该问题意味着当链路成本增加时，距离矢量路由算法需要很长时间才能收敛。 例如，考虑由三个节点 x、y 和 z 组成的网络。 假设链接成本最初是 c(x，y)=4，c(x，z)=50，c(y，z)=1。 距离矢量路由算法的结果表明，z 到 x 的路径是 z→y→x，代价是 5（=4+1）。 当链路(x，y)的成本从 4 增加到 60 时，需要 44 次迭代运行节点 z 的距离向量路由算法，才能认识到它对 x 的新的最小成本路径是通过它与 x 的直接链路，因此 y 也将实现它对 x 的最小成本路径是通过 z。【另外注意，解决“无穷计数”问题的方法是“毒性逆转技术”原书 P253，但环路上涉及三个或更多节点使用毒性逆转也无法检测到】

R6.每个自治系统使用相同的 AS 内部路由选择算法是必要的吗？说明原因。

答：不是。 每个 AS 具有在 AS 内路由的管理自主权。

R7.为什么在因特网中用到了不同的 AS 间与 AS 内部协议？

答：①策略——在多个 AS 之间，策略问题占主导地位。 很重要的是，来自指定 AS 的流量不能通过另一个指定 AS。 同样，指定的 AS 可能希望控制它在其他多个 AS 之间携带的过境交通。 在 AS 内部，所有的东西名义上都在相同的管理控制下，因此策略在选择 AS 中的路由方面的作用要小得多。 ②规模——路由算法及其数据结构对处理大量网络的路由的能力是 AS 间路由的一个关键问题。 在 AS 内部，可伸缩性不那么受关注。 首先，如果单个管理域变得太大，则始终可以将其划分为两个 AS 并在两个新的 AS 之间执行 AS 间路由。 ③性能——由于 AS 间路由是以策略为导向的，因此所使用的路由的质量(例如性能)往往是次要的问题(即满足某些策略标准的较长或更昂贵的路由很可能被接管到较短但不符合该标准的路由上)。 事实上，我们看到，在 AS 之间，甚至没有与路线相关的成本概念(除了 AS 跳数)。 然而，在单个 AS 中，这种策略关注的重要性较低，允许路由更多地关注在路由上实现的性能水平。

R8.判断：当一台 OSPF 路由器发送它的链路状态信息时，它仅向那些直接相邻的节点发送。解释理由。

答：错误。 使用 OSPF，路由器将其链路状态信息广播到它所属的自治系统中的所有其他路由器，而不仅仅是它的相邻路由器。 这是因为对于 OSPF，每个路由器需要构造一个完整的整个 AS 的拓扑图，然后本地运行 Dijkstra 的最短路径算法，以确定其到同一 AS 中所有其他节点的最小成本路径。

R9.在 OSPF 自治系统中，区域表示什么？为什么引入区域的概念？

答：在 OSPF 自治系统中的一个区域是指一组路由器，其中每个路由器将其链路状态广播到同一组中的所有其他路由器。 一个 OSPF 的 AS 可以分层配置成多个区域，每个区域运行自己的 OSPF 链路状态路由算法。 在每个区域内，一个或多个区域边界路由器负责在区域外路由数据包。 由于可伸缩性的原因，引入了区域的概念，即我们希望为大规模的 OSPF 的 AS 构建分层路由，而区域是分层路由中的一个重要构建块。

R10.定义和对比下列术语：子网、前缀和 BGP 路由。

答：子网是较大网络的一部分；子网不包含路由器；其边界由路由器和主机接口定义。 前缀是

CDIR 化地址的网络部分；它以 a.b.c.d/x 形式编写；前缀涵盖一个或多个子网。当路由器在 BGP 会话中发布前缀时，它包含了一些 BGP 属性。 在 BGP 术语中，前缀及其属性是 BGP 路由（或简单的路由）。【标准答案上写的就是 CDIRized address，有的题写的也是 CDIR，没查到是否是 CIDR 的同义表达】

R11.BGP 是怎样使用 NEXT-HOP 属性的？他是怎样使用 AS-PATH 属性的？
答：路由器的 AS-PATH 属性被用来在到同一前缀的多条路径中选择一条合适的；它也被用于检测和防止循环通告。 NEXT-HOP 属性指示沿通告路径(在接收通告的 AS 之外)到给定前缀的第一个路由器的 IP 地址。 在配置其转发表时，路由器使用 NEXT-HOP 属性。【这个问题下的"前缀"即在表示路由目的地，AS-PATH 的格式如"AS1, AS2, AS3"表示从 AS1 到 AS2 到 AS3，如果这条 AS-PATH 出现在 AS2 的路径列表中，AS2 会拒绝掉，因为包含自己表示这条路径成环了；NEXT-HOP 是 AS-PATH 上第一个 AS 的路由器接口的 IP 地址；一条 BGP 路由包括三个组件：NEXT-HOP、AS-PATH、目的前缀，事实上还有其他属性但属于超纲内容】

R13.是非判断题：当 BGP 路由器从它的邻居接收到一条通告的路径时，它必须对接收路径增加上它自己的标识，然后向其所有邻居发送该新路径。解释理由。
答：错误。 一个 BGP 路由器可以选择不将自己的标识添加到接收到的路径中，然后将该新路径发送给它的所有邻居，因为 BGP 是一种基于策略的路由协议。 这可能发生在以下场景中。接收到的路径的目的地是其他一些 AS，而不是 BGP 路由器的 AS，BGP 路由器不想作为传输路由器工作。

R19.列举 4 种不同的 ICMP 报文。
答：回显回答、目的网络不可达、目的主机不可达、目的端口不可达、源点抑制。【P273 包含全部类型，这里列几个好记的，其中"回显回答"是对 ping 命令的回复必须掌握，有的地方会写成"回送请求"，源点抑制涉及拥塞控制必须知道，这两个点防止出小题】

R20.发送主机执行 Traceroute 程序，收到哪两种类型的 ICMP 报文？
答：ICMP 警告报文（类型 11 代码 0）和目地端口不可达 ICMP 消息（类型 3 代码 3）。

P2.（P244 图 5-3）列举 x 到 z、z 到 u 以及 z 到 w 的不包含任何环路的路径。
答：x 到 z——x-y-z, x-y-w-z, x-w-z, x-w-y-z, x-v-w-z, x-v-w-y-z, x-u-w-z, x-u-w-y-z, x-u-v-w-z, x-u-v-w-y-z；z 到 u——z-w-u, z-w-v-u, z-w-x-u, z-w-v-x-u, z-w-x-v-u, z-w-y-x-u, z-w-y-x-v-u, z-y-x-u, z-y-x-v-u, z-y-x-w-u, z-y-x-w-y-u, z-y-x-v-w-u, z-y-w-v-u, z-y-w-x-u, z-y-w-v-x-u, z-y-w-x-v-u, z-y-w-y-x-u, z-y-w-y-x-v-u；z 到 w——z-w, z-y-w, z-y-x-w, z-y-x-v-w, z-y-x-u-w, z-y-x-u-v-w, z-y-x-v-u-w。【注意路径含首尾】

P3.【P279，下为原书编者的迪杰斯特拉算法计算最短路径的答题格式】
答：

Step	*N'*	*D(t),p(t)*	*D(u),p(u)*	*D(v),p(v)*	*D(w),p(w)*	*D(y),p(y)*	*D(z),p(z)*
0	x	∞	∞	3,x	6,x	6,x	8,x
1	xv	7,v	6,v	3,x	6,x	6,x	8,x
2	xvu	7,v	6,v	3,x	6,x	6,x	8,x
3	xvuw	7,v	6,v	3,x	6,x	6,x	8,x
4	xvuwy	7,v	6,v	3,x	6,x	6,x	8,x
5	xvuwyt	7,v	6,v	3,x	6,x	6,x	8,x
6	xvuwytz	7,v	6,v	3,x	6,x	6,x	8,x

【注意是从 x 出发，所有权值都是计算结点到 x 的距离而不是结点到生成树的距离，p 的值为生成树上直接与本结点相连的那个结点】

P5.【P279，下为原书编者的 RIP 路由表项答题格式】

答:

①

		Cost to u	v	x	y	z
From	v	∞	∞	∞	∞	∞
	x	∞	∞	∞	∞	∞
	z	∞	6	2	∞	0

②

		Cost to u	v	x	y	z
From	v	1	0	3	∞	6
	x	∞	3	0	3	2
	z	7	5	2	5	0

③

		Cost to u	v	x	y	z
From	v	1	0	3	3	5
	x	4	3	0	3	2
	z	6	5	2	5	0

④

		Cost to u	v	x	y	z
From	v	1	0	3	3	5
	x	4	3	0	3	2
	z	6	5	2	5	0

P6.考虑一个一般性拓扑（即没有指定任何结构的网络）和一个同步版本的距离向量算法。假设每次迭代时，一个节点与其邻居交换其距离向量并接受他们的距离向量。假定算法开始时，每个节点只知道其直接邻居的开销，在该分布式算法收敛前所需的最大迭代次数是多少？

答：这个问题的措辞有点模棱两可。 我们的意思是，“第一次运行算法时的迭代次数”（也就是说，假设节点最初拥有的唯一信息是它们最近邻居的成本）。 我们假设算法同步运行（即在一步中，所有节点同时计算它们的距离表，然后交换表）。

在每次迭代中，节点与其邻居交换距离表。 因此，如果您是节点 A，并且您的邻居是 B，那么 B 的所有邻居（它们都将是您的一到两个跳）都将知道在一次迭代之后(即在 B 告诉它们它对您的成本之后)给您的最短成本路径。

设 d 是网络的“直径”——网络中任意两个节点之间没有回路的最长路径的长度。 使用上面的推理，经过 d-1 迭代后，所有节点将知道 d 或更少跳到所有其他节点的最短路径成本。 由于任何大于 d 跳的路径都将具有循环（因此比删除循环的路径具有更大的成本），因此该算法将在最多 d-1 迭代中收敛。

ASIDE：如果 DV 算法是由于链路成本的变化而运行的，则在收敛之前，对所需的迭代次数没有先验约束，除非还指定了链路成本的约束。

P8.【P251 图 5-6 上】不用显示在图中的开销，链路开销值现在是 c(x, y)=3，c(y, z)=6，c(z, x)=4。计算在距离向量表初始化后，以及在同步版本的距离向量算法收敛后的距离向量表。

答:

Node x table

		Cost to x	Cost to y	Cost to z
From	x	0	3	4
	y	∞	∞	∞
	z	∞	∞	∞

		Cost to x	Cost to y	Cost to z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

Node y table

		Cost to x	Cost to y	Cost to z
From	x	∞	∞	∞
	y	3	0	6
	z	∞	∞	∞

		Cost to x	Cost to y	Cost to z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

Node z table

		Cost to x	Cost to y	Cost to z
From	x	∞	∞	∞
	y	∞	∞	∞
	z	4	6	0

		Cost to x	Cost to y	Cost to z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

P9.考虑距离向量路由选择中的无穷计数问题，如果我们减少一条链路的开销，将会出现无穷计数问题吗？为什么?如果我们将没有链路的两个节点连接起来，会出现什么情况?
答: 不会, 这是因为降低链接成本不会导致循环(由该链接的两个节点之间的下一跳关系引起)。将两个节点与一个链路连接起来，相当于将链路权重从无限减小到有限权重。

P11.【题目 P280，图片 P252 图 5-7，题目要求对毒性逆转在何时有效何时无效有彻底掌握】
答: a.

Router z	Informs w, $D_z(x)=\infty$
	Informs y, $D_z(x)=6$
Router w	Informs y, $D_w(x)=\infty$
	Informs z, $D_w(x)=5$
Router y	Informs w, $D_y(x)=4$
	Informs z, $D_y(x)=4$

【采取毒性逆转技术时，节点只会告诉下一跳结点自己到目的节点不可达，而对于路径上的非下一跳节点仍然会告诉它自己到目的节点的距离】

b. 是的，会有一个“无穷计数”的问题。 下表显示了路由汇聚过程。 假设在 t_0 时，链路成本发生变化。 在 t_1 时，y 更新其距离向量并通知邻居 w 和 z。 在下表中，“→”代表“通知”。

time	t0	t1	t2	t3	t4
Z	→ w, $D_z(x)=\infty$ → y, $D_z(x)=6$		No change	→ w, $D_z(x)=\infty$ → y, $D_z(x)=11$	
W	→ y, $D_w(x)=\infty$ → z, $D_w(x)=5$		→ y, $D_w(x)=\infty$ → z, $D_w(x)=10$		No change
Y	→ w, $D_y(x)=4$ → z, $D_y(x)=4$	→ w, $D_y(x)=9$ → z, $D_y(x)=\infty$		No change	→ w, $D_y(x)=14$ → z, $D_y(x)=\infty$

我们看到 w，y，z 在计算路由器 x 的成本时形成了一个循环。 如果我们继续上表所示的迭代，那么我们将看到，在 t27，z 通过它与 x 的直接链接检测到它对 x 的最小成本是 50。 在 t29，w 通过 z 学习它对 x 的最小成本是 51。 在 t30，y 将其最小成本更新为 x 为 52(通过 w)。 最后，在时间 t31，没有更新，路由稳定。

time	t27	t28	t29	t30	t31
Z	→ w, $D_z(x)=50$ → y, $D_z(x)=50$				via w, ∞ via y, 55 via z, 50
W		→ y, $D_w(x)=\infty$ → z, $D_w(x)=50$	→ y, $D_w(x)=51$ → z, $D_w(x)=\infty$		via w, ∞ via y, ∞ via z, 51
Y		→ w, $D_y(x)=53$ → z, $D_y(x)=\infty$		→ w, $D_y(x)=\infty$ → z, $D_y(x)=52$	via w, 52 via y, 60 via z, 53

c. 切断 y 和 z 之间的联系。

P14.【P280】

答：四题的顺序依次是 eBGP、iBGP、eBGP、iBGP。【只要是路由器知道了自己 AS 以外的路由情况就是通过 BGP 协议，只有自己 AS 内的路由情况才用 RIP 或 OSPF，在 AS 内部用 BGP 传阅时使用 iBGP，在 AS 的各个发言人之间使用 BGP 传阅用 eBGP】

第六章

R2.如果因特网中所有链路都提供可靠交付，TCP 可靠传输服务是多余的吗？为什么？

答：虽然每个链路都保证通过链路发送的 IP 数据报将在链路的另一端收到，而不会出现错误，但不能保证 IP 数据报将以适当的顺序到达最终目的地。 有了 IP，在同一 TCP 连接中的数据报可以在网络中采取不同的路由，因此无法正常到达。 仍然需要 TCP 以正确的顺序为应用程序的接收端提供字节流。此外, IP 还可能由于路由循环或设备故障而丢失数据包。【即仍需要 TCP 的可靠传输解决数据报乱序的问题】

R3.链路层协议能够向网络层提供哪些服务？在这些链路层服务中, 哪些在 IP 中有对应的服务？哪些在 TCP 中有对应的服务？

答：封装成帧：IP 和 TCP 中也有封装 MTU 的功能；链路接入；可靠交付：TCP 中也有可靠交付；流量控制：TCP 中也有流量控制；差错检测：IP 和 TCP 中也有差错检测；纠错；全双工：TCP 也是全双工。【答案一共写了七种功能，P287 只写了五种，流量控制和全双工通信没写，其中 TCP 可以实现 4 种，IP 可以实现 2 种】

R5.广播信道的四种希望特性中，哪些是时隙 ALOHA 所具有的？令牌传递具有这些特性中的哪些？

答：时隙 ALOHA：1, 2 和 4(时隙 ALOHA 仅部分分散，因为它需要所有节点中的时钟同步)。令牌环网：1, 2, 3, 4。【P294 具体写了四条特性，这里简单概述：1.当仅有一个节点发送数据时，该结点具有全部吞吐量；2.当有多个节点发送数据时，各节点均分吞吐量；3.协议是分散的，不会因为某主节点故障而导致系统崩溃；4.协议是简单的，能够轻易实现】

R6.在 CSMA/CD 中，第五次碰撞后，节点选择 K=4 的概率有多大？结果 K=4 在 10Mbps 以太网上对应于多少秒的时延？

答：在第 5 次碰撞后，适配器从{0、1、2、...、31}中选择。 它选择 4 的概率是 1/32。 它等待 204.8 微秒。【指数规避算法下，第 n 次碰撞就在2^n个数中选一个作为退避时间，数字从 0 开始】

R8.如果局域网有很大的周长时，为什么令牌环协议将是低效的？

答：当节点发送帧时，节点必须等待帧围绕整个环传播到达目的地，然后节点才能释放令牌。因此，如果 L/R 比 t_{prop} 小，那么协议将是低效的。

R9.MAC 地址空间有多大？IPv4 呢？IPv6 呢？

答：2^{48} MAC；2^{32} IPv4；2^{128} IPv6。

R10.若节点 A, B, C 通过适配器连接到同一个广播局域网上。此时 A 向 B 发送 IP 数据报，每个帧都封装了 B 的 MAC 地址，C 的适配器会处理这些帧吗？如果会，C 的适配器会把帧传递给 C 的网络层吗？若 A 用 MAC 广播地址来发送这些帧又如何？

答：C 的适配器会处理 A 发送的帧但不会传递给 C 的网络层；若用广播地址则 C 的适配器会接收 A 发送的帧且传递给 C 的网络层。

R11.ARP 查询为什么要在广播帧中发送呢？ARP 响应为什么要在一个具有特定目的 MAC 地址的帧中发送呢？

答：在广播帧中发送 ARP 查询，因为查询主机与所述 IP 地址不对应。 对于响应，发送节点知道响应应该发送到的适配器地址，因此不需要发送广播帧（它必须由局域网上的所有其他节点处理）。【即查询时，主机不知道目的主机的地址，于是广播一个帧，谁知道谁回应，而回复时，发送回复的主机可以从查询帧中找出对方的 MAC 地址，因此不需广播帧】

P1.对 1110 0110 1001 1101 使用偶校验方案，在采用二维奇偶校验方案的情况下，包含该检验比特的字段值是多少？回答应使用最小长度检验和字段。

答：
1 1 1 0 1
0 1 1 0 0
1 0 0 1 0
1 1 0 1 1
1 1 0 0 0

【把原比特序列写成矩阵形式，然后在行末和列末添加校验位】
【奇方案偶方案看的是 1 的个数是奇数还是偶数】

P2.说明（举一个不同于 P290 图 6-5 的例子）二位奇偶校验能够纠正和检验单比特差错。说明（任举一个例子）某些双比特差错能够被检测但不能纠正。

答：

正确的校验和矩阵 A	$a_{2,3}$ 出错	$a_{2,2}$ 和 $a_{2,3}$ 同时出错
0 0 0 0	0 0 0 0	0 0 0 0
1 1 1 1	1 1 0 1	1 0 0 1
0 1 0 1	0 1 0 1	0 1 0 1
1 0 1 0	1 0 1 0	1 0 1 0

【总之，假设校验位本身不出错的情况下，单比特校验一定无法发现偶位比特差错，双比特校验一定能发现偶位比特差错，但如果错误发生在同一行/列，则无法纠正】

P5.考虑 5 比特生成多项式，G=10011，并假设 D 的值为 1010101010。问 R 的值是多少？

答：结果为 1010101010 0100。【余数为 0100，循环冗余校验必须会，方法见 P292 瘫痪级教程】

P6.仍对于上一题而言，G 不变继续练习三道题。

a.D=1001010101

答：1001010101 0000【考试时中间不必空开，或者数字之间间隔有规律方便阅卷老师】

b.D=0101101010

答：0101101010 1111【首位不为零则从下一位开始算】

c.D=1010100000

答：1010100000 1001

P8.【P332】

答：

a.

$$E(p) = Np(1-p)^{N-1}$$

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

$$= N(1-p)^{N-2}((1-p) - p(N-1))$$

$$E'(p) = 0 \Rightarrow p^* = \frac{1}{N}$$

b.

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

$$\lim_{N\to\infty}(1-\frac{1}{N}) = 1 \qquad \lim_{N\to\infty}(1-\frac{1}{N})^N = \frac{1}{e}$$

Thus

$$\lim_{N\to\infty} E(p^*) = \frac{1}{e}$$

P9.说明纯 ALOHA 最大效率是（1/2e）。

答:

$$E(p) = Np(1-p)^{2(N-1)}$$

$$E'(p) = N(1-p)^{2(N-2)} - Np2(N-1)(1-p)^{2(N-3)}$$

$$= N(1-p)^{2(N-3)}((1-p) - p2(N-1))$$

$$E'(p) = 0 \Rightarrow p^* = \frac{1}{2N-1}$$

$$E(p^*) = \frac{N}{2N-1}(1-\frac{1}{2N-1})^{2(N-1)}$$

$$\lim_{N\to\infty} E(p^*) = \frac{1}{2}\cdot\frac{1}{e} = \frac{1}{2e}$$

P15.（P333）

答: a. 不会。 可以检查主机 F 的 IP 地址的子网前缀，然后了解 F 在同一个局域网上。 因此，E 不会将数据包发送到默认路由器 R1。 以太网帧从 E 到 F：源 IP=E 的 IP 地址、目的 IP=F 的 IP 地址、源 MAC=E 的 MAC 地址、目的地 MAC=F 的 MAC 地址。

b. 不会。 通过检查 B 的 IP 地址，E 可以发现目的 IP 不在同一网络下。 以太网帧从 E 到 R1：源 IP=E 的 IP 地址、目的 IP=B 的 IP 地址、源 MAC=E 的 MAC 地址、目的地 MAC=连接到子网 3 的 R1 接口的 MAC 地址。

c. 【注意 S1 的所指，图中子网 1 和子网 2 中间那个路由器被题干换成了交换机，这个交换机是 S1】①交换机 S1 将通过其两个接口广播以太网帧，因为接收到的 ARP 帧的目标地址是广播地址。 它了解到 A 通过 S1 面向子网 1 的接口，连接到 S1 上，并且 S1 将更新其转发表，以包含主机 A 的条目。②是的，路由器 R1 也接收这个 ARP 请求消息，但是 R1 不会将消息转发到子网 3。③B 不会发送 ARP 查询消息来要求 A 的 MAC 地址，因为这个地址可以从 A 的查询消息中获得。④一旦交换机 S1 接收到 B 的响应消息，它将在其转发表中为主机 B 添加一个条目，然后将接收到的帧删除，因为目标主机 A 与主机 B 在同一接口上(即 A 和 B 在同一局域网段上)。【注意 A 的帧中是广播 MAC 地址，S1 收到帧后是不会阻断广播帧的广播的，因此①中 S1 会通过两个接口转发，而在④中 S1 收到的帧目的地址明确是 A 的 MAC 地址，因此 S1 不会转发到右边】

第七章

R1.一个无线网络运行在“基础设施模式”下是什么含义？如果网络没有运行在基础设施模式下那它运行在什么模式下？这种运行模式与基础设施模式之间有什么关系？

答：在基础设施运行模式下，每个无线主机通过基站(接入点)连接到更大的网络。 如果不以基础设施模式运行，则以自组织网络模式运行。在自组织网络下，无线主机没有连接的基础设施。在这种无基础设施的情况下，主机本身必须提供路由、地址分配、类似 DNS 的名称转换等服务。

R2.四种无线网络类型各是什么？你正在使用的是哪一种？

答：基于基础设施的单跳、无基础设施的单跳、基于基础设施的多跳、无基础设施的多跳。【原书主要以基于基础设施的单跳和多跳为内容，生活中一般是基于基础设施的单跳】

R3.下列类型的无线信道损伤之间有什么区别：路径损耗、多径传播、来自其他源的干扰。

答：路径损耗是由于电磁信号在穿过物质时发生衰减。 多路径传播会导致接收端接收信号的模糊，电磁波的一部分在物体和地面之间反射时，会在发送端和接收方之间形成不同长度的路径。来自其他源的干扰会在两个源以同一频段发送信号时发生，这两个源的电波将相互干扰。

R4.随着移动节点距离基站越来越远，为保证传送帧的丢失概率不增加，基站能够采取的两种措施是什么？

答：增加传输功率；降低传输速率。

R5.描述 802.11 中信标帧的作用。

答：接入点（AP）发射信标帧。 一个 AP 的信标帧将通过 11 个信道中的一个传输。 信标帧允许附近的无线设备发现和识别 AP。

R6.是非判断：802.11 在传输一个数据帧前，必须首先发送一个 RTS 帧并接收一个对应 CTS 帧。

答：错误。【使用 RTS 和 CTS 解决隐蔽站问题是可选的而非必须，长数据帧才使用 RTS，见 R9】

R7.为什么 802.11 中使用了确认，而有线以太网中却未使用？

答：标准答案缺失。【因为 802.11 使用的是 CSMA/CA 碰撞避免而非有线以太网中的 CSMA/CD 碰撞检测，碰撞避免无法“边发边听”，一旦发送无法停止直到发完整个帧，因此无法保证所发送的帧完好无损的到达接收方，于是引入了确认和超时重传机制。P350、P352】

R8.是非判断：以太网和 802.11 使用相同的帧格式。

答：错误。【有很多相似，但无线网络有专属字段。P353】

R9.描述 RTS 门限值的工作过程。

答：每个无线站可以设置一个 RTS 阈值，以便只有当要传输的数据帧大于阈值时才使用 RTS/CTS 序列。 这确保了 RTS/CTS 机制仅用于长数据帧。

R10.假设 802.11RTS 和 CTS 帧与标准的 DATA 和 ACK 帧一样长，使用 CTS 和 RTS 还会有好处吗？为什么？

答：不，没有任何优势。 假设有两个站希望同时传输，它们都使用 RTS/CTS。 如果 RTS 框架与 DATA 框架一样长，则发送帧的通道将可能在不断的碰撞中被长时间浪费。 因此，只有当 RTS/CTS 帧明显小于 DATA 帧时，RTS/CTS 交换才是有用的。

R11.无线站点从一个 BSS 到同一子网中的另一个 BSS。当 AP 是通过交换机互联时，为了让交换机能适当的转发帧，一个 AP 可能需要发送一个带有哄骗的 MAC 地址帧，为什么？

答：最初，交换机的转发表中有一个条目，该条目将无线站与先前的 AP 关联起来。当无线站与新 AP 关联时，新 AP 将创建一个带有无线站 MAC 地址的帧并广播该帧。帧被交换机接收。这将迫使交换机更新其转发表，以便发送到无线站的帧通过新的 AP 发送。

R12.蓝牙网络中的主设备和 802.11 网络中的一个基站有何不同？
答：任何普通的蓝牙节点都可以是主节点，而 802.11 网络中的接入点是特殊的设备（普通的无线设备，如笔记本电脑，不能用作接入点）。

R13.在 802.15.4ZigBee 标准中，超级帧的含义是什么？
答：答案缺失。【P358，以下为概述：超帧由信标定义，由主协调器发送用于控制多个简化功能设备，超帧被分为 16 个大小相等的时隙，其中，第一个时隙为信标。信标在每一个超帧的第一个时隙中进行传输，如果主设备不使用超帧结构，那么它将关掉信标的传输。】

R14.3G 蜂窝体系中的“核心网”是什么？
答：答案缺失。【3G 核心蜂窝数据网将无线电接入网连接到公共因特网，核心网包括 SGSN 和 GPRS，SGSN 负责向位于其连接的无线电接入网的移动节点交付数据包，GGSN 起着网关的作用，将多个 SGSN 连接到更大的因特网。】

R17.3G 和 4G 的三个重要差别是什么？
答：①在 3G 体系结构中，语音和数据有单独的网络组件和路径，即语音通过公共电话网络，而数据通过公共互联网。 4G 体系结构是一种统一的全 IP 网络体系结构，即语音和数据都是在 IP 数据报中传输到/从无线设备到多个网关，然后传输到 Internet 的其余部分。②4G 网络架构清晰地将数据和控制平面分开，与 3G 架构不同。③4G 架构具有增强的无线电接入网络(E-UTRAN)，不同于 3G 的无线电接入网络 UTRAN。【5G 与 4G 的区别极简地概括一下就是高速度、高并发】

R18.如果某节点与因特网具有无线连接，则该节点必定是移动的吗？试解释之。假设一个使用笔记本电脑的用户携带电脑绕着她的住所散步，而且总是通过相同的接入点接入因特网。从网络的角度看，这是移动用户吗？试解释之。
答：不是。 一个节点可以在接入 Internet 的整个持续过程中始终维持同一个接入点的连接（因此，不一定是移动的）。 移动节点是随着时间的推移将其附着点更改为网络的节点。 由于用户总是通过同一个接入点访问互联网，所以她不是移动的。

R19.永久地址与转交地址之间的区别是什么？谁指派转交地址？
答：移动节点的永久地址是它在其主网络时的 IP 地址。 当它访问一个外部网络时，它得到的是转交地址。由外部代理（可以是外部网络中的边缘路由器，也可以是移动节点本身）分配 COA。

R20.考虑经移动 IP 的一条 TCP 连接。是非判断：在通信者和移动主机之间的 TCP 连接阶段经过该移动用户的归属网络，但数据传输阶段是直接通过该通信者和移动主机，绕开了归属网络。
答：错误。【在间接路由选择中 P368，通信者是直接与归属代理建立 TCP 连接以及传输数据的，当然移动主机对通信者发送报文时，连接是在二者之间的；在直接路由选择中 P370，包括使用锚外部代理方案，通信者都是通过通信者代理询问得到移动主机 COA 后，再由通信者代理与移动主机或锚外部代理建立 TCP 连接的，两种方法均没有通信者与移动主机之间直接传输数据】

R21.在 GSM 网络中，HLR 和 VLR 的目的是什么？移动 IP 的什么要素类似于 HLR 和 VLR？
答：①GSM 中的家庭网络维护一个名为家庭位置寄存器(HLR)的数据库，该数据库包含其每个订阅者的永久手机号码和订阅者配置文件信息。 HLR 还包含有关这些订户当前位置的信息。

访问的网络维护一个称为访问者位置寄存器(VLR)的数据库，该数据库包含当前位于 VLR 服务的网络部分的每个移动用户的条目。 因此，随着移动用户进出网络，VLR 条目因此进出。②移动 IP 中的家庭网络中的边缘路由器与 GSM 中的 HLR 相似，国外网络中的边缘路由器与 GSM 中的 VLR 相似。

R22.在 GSM 网络中，锚 MSC 的作用是什么？
答：锚 MSC 是手机在呼叫开始时访问的 MSC；锚 MSC 因此在呼叫期间保持不变。 在整个呼叫的持续时间内，无论移动设备执行的 MSC 之间传输的数量如何，呼叫从主 MSC 路由到锚 MSC，然后从锚 MSC 路由到移动设备当前所在的访问 MSC。

P1.考虑在 P344 图 7-5 中单一发送方的 CDMA 例子，如果发送方的 CDMA 码是（1, -1, 1, -1, 1, -1, 1, -1），那么其输出（对于所显示的两个数据比特）是什么？
答：d_1=[-1, 1, -1, 1, -1, 1, -1, 1]；d_0=[1, -1, 1, -1, 1, -1, 1, -1]。

P2.考虑在 P346 图 7-6 中的发送方 2，发送方 2 对信道$Z_{i,m}^2$的输出是什么（在它被加到来自发送发 1 的信号前）？
答：d_1=[1,-1,1,1,1,-1,1,1]；d_0=[1,-1,1,1,1,-1,1,1]。

P3.考虑在 P346 图 7-6 中的接收方，演示接收方通过接收到的信号还原出发送方 2 数据内容的计算过程。
答：

$$d_2^1 = \frac{1\times1+(-1)\times(-1)+1\times1+1\times1+1\times1+(-1)\times(-1)+1\times1+1\times1}{8} = 1$$

$$d_2^2 = \frac{1\times1+(-1)\times(-1)+1\times1+1\times1+1\times1+(-1)\times(-1)+1\times1+1\times1}{8} = 1$$

【还原数据即将接收内容与编码逐位相与然后计算各个位的平均值】

P13.在移动 IP 中，移动性将对数据报在源和目的地间的端到端时延有何影响？
答：因为数据报必须首先转发到归属代理，然后从那里转发到移动，所以延迟通常比通过直接路由要长。 但是，请注意，从通信者到移动主机的直接延迟（即，如果数据报不是通过主代理路由的）实际上可能小于从通信器到主代理和从那里到移动器的延迟之和。 这将取决于这些不同路径段的延迟。 此外，间接路由还增加了主代理处理（例如封装）延迟

P16.在我们对 VLR 如何用移动用户当前位置信息更新 HLR 的讨论中，与 VLR 地址对 HLR 对比，提供 MSRN 所具有的优缺点是什么？
答：如果将 MSRN 提供给 HLR，那么每当 MSRN 发生变化时(例如，当有需要 MSRN 更改的切换时)，必须在 HLR 中更新 MSRN 的值。 在 HLR 中具有 MSRN 的优点是可以快速提供该值，而无需查询 VLR。 通过提供 VLR 的地址而不是 MSRN，没有必要刷新 HLR 中的 MSRN。

第八章

R1.报文机密性和报文完整性之间的区别是什么？你能具有机密性而没有完整性吗？你能具有完整性而没有机密性吗？证实你的答案。

答：具有机密性需要满足，原始明文消息无法由试图截取内容的攻击者确定。具有完整性需要满足，接收方可以检测发送的消息(无论是否加密)在传输过程中是否被更改的属性。因此，这两者是不同的概念，可以有一个而没有另一个。在传输中被更改的加密消息可能仍然是机密的(攻击者不能确定原始明文)，但如果错误未被检测到，则不会具有消息完整性。类似地，在传输过程中被更改(并被检测到)的消息可能是以明文发送的，因此不属于机密。【机密性即不可被阅读，完整性即不可被更改。或者说的准确一点完整性是能够检测出消息是否被更改，被更改则丢弃】

R3.从服务的角度，对称密钥系统和公开密钥系统之间的一个重要差异是什么？

答：对称密钥系统和公钥系统之间的一个重要区别是，在对称密钥系统中，发送方和接收方都必须知道相同但保密的密钥。在公钥系统中，加密密钥和解密密钥是不同的。整个世界(包括发送方)都知道加密密钥，但是解密密钥只有接收方知道。

R6.假定 N 个人中，每个人都和其他 N-1 个人使用对称密钥密码通信。在任意两人之间的所有通信对其他人都是可见的。该组中的其他人都不应当能解密他们的通信，则这个系统共需要多少个密钥？假定使用公开密钥密码，此时需要多少个密钥？

答：如果每个用户希望与 N 个其他用户通信，那么每对用户必须具有一个共享的对称密钥。有 N*(N-1)/2 个这样的对，因此有 N*(N-1)/2 个密钥。对于公钥系统，每个用户都有一个所有人都知道的公钥和一个私钥(私钥是秘密的，只有用户知道)。因此，在公钥系统中有 2N 个密钥。

R7.假设 n=10000、a=10023 和 b=10004。请你使用等同的模算术来心算(a*b)mod n。

答：a mod n = 23 , b mod n = 4。所以(a*b) mod n = 23*4=92。

R9.散列以何种方式提供比检验和更好的报文完整性检验？

答：消息摘要的要求是，给定消息 M，很难找到具有相同消息摘要的另一个消息 M'，且作为推论，给定消息摘要值很难找到具有给定消息摘要值的消息 M"。我们拥有"消息完整性"，因为我们有理由相信，给定消息 M 及其签名的消息摘要，自计算和签名消息摘要以来，该消息没有被更改。Internet 校验和则不是这样，我们在图 7.18 中看到，很容易找到具有相同 Internet 校验和的两条消息。【总的来说，使用检验和是有较大概率出现检验和无法发现消息被更改的情况的，而使用散列函数则很难有另一组数字与真实内容被散列过后的结果相同，因此更能保证消息完整性】

R10.你能够"解密"某报文的散列来得到初始报文吗？

答：不能。这是因为哈希函数是单向函数。也就是说，给定任何散列值，原始消息都无法恢复(给定 h，如果 h= H (m)，则无法从 h 中恢复 m)。【因此数字签名的验证过程中是将明文经过数据中一起传过来的散列函数处理后，比较处理结果和签名内容，而不是拿签名内容反求明文】

R11.如 P399 图 8-9，考虑 MAC（报文鉴别码）算法的一种变形算法，其中发送方发送（m, H(m)+s），这里的 H(m)+s 是 H(m)和 s 的级联。该变形算法有缺陷吗？为什么？

答：这个计划显然有缺陷。Trudy 是一个攻击者，它可以先嗅探通信，然后从 H(m)+s 中提取最后一部分数字，从而获得共享的秘密 s。然后，Trudy 可以通过创建自己的消息 t 来伪装成发送者，并发送(t, H(t)+s)。【P399 图 8-9 是报文鉴别码方案的概括精华，或见习题 P12 答案更详实】

R12.一个签名的文档是可鉴别的和不可伪造的，含义是什么？

答：假设 Bob 向 Alice 发送了一个加密的文档。何谓可鉴别，Alice 必须能确信是 Bob 发送的加密的文档。何谓不可伪造，Alice 必须能确信只有 Bob 发送了加密文档(例如，没有其他人能够猜到密钥并加密/发送文档)。为了说明后一种区别，假设 Bob 和 Alice 共享一个密钥，并且他们是世界上唯一知道该密钥的人。如果 Alice 收到一个用密钥加密的文档，并且知道她自己没有加密文档，那么就知道该文档是可验证的和不可伪造的(假设使用了适当强的加密系统)。然而，Alice 不能说服其他人 Bob 一定发送了文档，因为事实上 Alice 自己知道密钥，并且可能已经加密/发送了文档。

R13.公钥加密的报文散列以何种方式比使用公钥加密报文提供更好的数字签名？
答：使用公钥加密的报文散列“更好”，因为只需要加密(使用私钥)散列报文，而不需要加密整个消息。由于使用像 RSA 这样的技术进行公钥加密是昂贵的，因此需要签署(加密)较小数量的数据而不是较大数量的数据。【题里说的“公钥加密的”意思是指使用公钥私钥方案，而不是说发送方用公钥对报文散列加密，**P409 图 8-19、8-20、8-21 非常重要**，是公钥私钥方案的图像总结，图 8-21 的右半部分接收过程在**习题 P.17**】

R14.假设 certifier.com 生成一个用于 foo.com 的证书。通常整个证书将用 certifier.com 的公钥加密。这种说法是正确还是错误？
答：这是错误的。要创建证书，certifier.com 将包含一个数字签名，它是 foo.com 信息(包括其公钥)的散列，并使用 certifier.com 的私钥签名。【数字签名的加密用私钥，接收方的解密用公钥】

R15.假设 Alice 有一个准备发送给任何请求者的报文。数以千计的人想要获得 Alice 的报文，但每个人都要确保该报文的完整性。在这种情况下，你认为是基于 MAC 还是基于数字签名的完整性方案更合适？为什么？
答：对于基于 MAC 的方案，Alice 必须与每个潜在的接收者建立一个共享密钥。有了数字签名，她为每个收件人使用相同的数字签名；数字签名是通过使用她的私钥对消息的散列进行签名而创建的。在这里，数字签名显然是更好的选择。【注意图 8-9 中的 s 是双方都要持有的，这就要求 Alice 必须保持这数以千计的共享秘密，而图 8-20、21 中，加密解密方没有必需同时持有的内容，只需为每一个报文确定一个数字签名即可】

R16.在某端点鉴别协议中，使用不重数的目的是什么？
答：防止回放攻击。【P406】

R17.我们说一个不重数是一个在生存期中只使用一次的值，这意味着什么？是指谁的生存期？
答：一次生存期意味着发送该不重数的实体将不再使用该值来检查另一个实体是否“活动”。【使用不重数的过程：①Alice 发送给 Bob 一个消息；②Bob 发送不重数；③Alice 使用对称密钥加密不重数发回给 Bob。于是 Bob 知道了两件事：1.对方是 Alice 因为使用了对称密钥；2.Alice 是活跃的因为发送不重数获得了响应。生存周期是这个协议的周期，P406 原话】

R20.在 SSL 记录中，有一个字段用于 SSL 序号。这种说法正确还是错误？
答：错误。SSL 使用隐式序列号。

R21.在 SSL 握手中，使用不重数的目的是什么？
答：不重数用于防御“连接重放攻击”。【序号用于防御在一个进行中的会话中，重放个别分组】

R29.状态分组过滤器维护两个数据结构。给出它们的名字并简单讨论其功能。
答：过滤表和连接表。连接表跟踪连接，允许更精细的报文过滤。【过滤表用于给分组过滤器提

供过滤规则，据此决定收到的数据报该允许通过还是丢弃】

R30.考虑某传统的（无状态的）分组过滤器。该分组过滤器可能基于 TCP 标志位以及其他首部字段过滤分组。这种说法正确还是错误?
答：正确。【也就是 P426 表 8-6 的"标志比特"，通常用于限制外来报文仅允许 ACK 通过】

R31.在传统的分组过滤器中，每个接口能够具有自己的访问控制表。这种说法正确还是错误?
答：正确。

R32.为什么应用程序网关必须与分组过滤器协同工作才有效?
答：如果没有分组过滤器，那么机构网络内的用户仍然能够与机构网络外的主机直接连接。过滤器强制用户首先连接到应用程序网关。【P428 图 8-34，应用程序网关用于检查 IP/TCP/UDP 首部（同时过滤器也可以完成）并检查其中的应用数据（过滤器无法完成），当内网要向外发起连接时，过滤器迫使连接经过应用程序网关】

R33.基于特征的 IDS 和 IPS 检查 TCP 和 UDP 报文段的载荷。该说法正确还是错误?
答：正确。

P8.考虑 p=5 和 q=11 的 RSA。

a.n 和 z 是什么?

答：n = p*q = 55；z = (p-1)(q-1) = 40。

b.令 e 为 3。为什么这是一个对 e 的可接收的选择?

答：e = 3 小于 n 以及 e = 3 与 z 没有公因式。

c.求 d 使得 de=1(mod z)和 d<160。

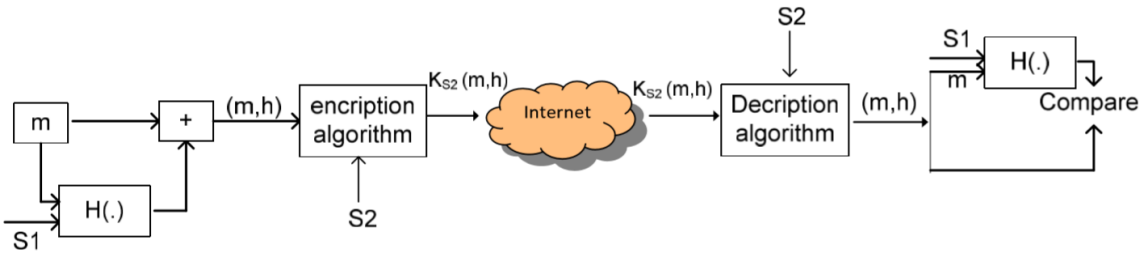
答：d = 27。

d.使用密钥(n, e)加密报文 m=8.令 c 表示对应密文。显示所有工作。提示：为了简化计算，使用如下事实：

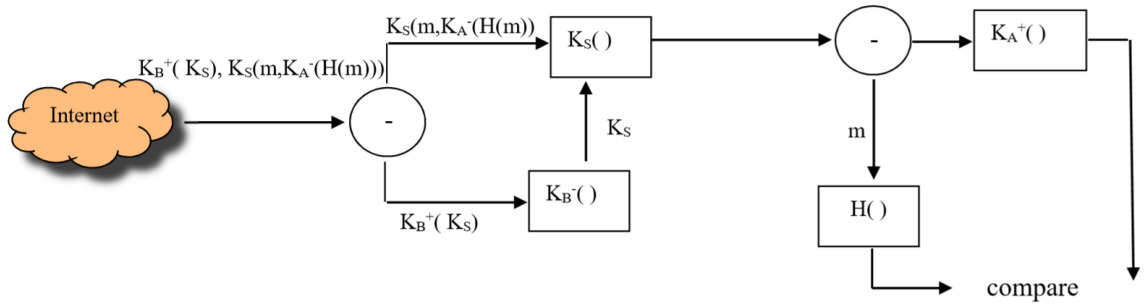
$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$

答：m = 8，me = 512，密文 c= me mod n = 17。

P12.Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充 P399 图 8-9 使之提供完整性和机密性。
答：



P17.图 8-19 显示了 Alice 必须执行 PGP 操作，以提供机密性、鉴别和完整性。图示出 Bob 接收来自 Alice 的包时必须执行的对应操作。
答：



P25.对尽可能限制但能实现下列功能的一台有状态防火墙，提供一张过滤表和连接表。

a.允许所有内部用户与外部用户创建 Telnet 会话。

b.允许外部用户访问公司位于 222.22.0.12 的 Web 站点。

c.否则阻挡所有入流量和出流量。

内部网络号为 222.22/16。在你的答案中，假设连接表当前缓存了 3 个从内向外的连接。需要虚构适当的 IP 地址和端口号。

答: 过滤表——

Action	Source Address	Dest address	Protocol	Source port	Dest port	Flag bit	Check connection
allow	222.22/16	outside of 222.22/16	TCP	> 1023	23	any	
allow	outside of 222.22/16	222.22/16	TCP	23	> 1023	ACK	X
Allow	outside of 222.22/16	222.22.0.12	TCP	>1023	80	Any	
Allow	222.22.0.12	outside of 222.22/16	TCP	80	>1023	Any	
deny	All	all	all	all	all	All	

连接表——

Source address	Dest address	Source port	Dest port
222.22.1.7	37.96.87.123	12699	23
222.22.93.2	199.1.205.23	37654	23
222.22.65.143	203.77.240.43	48712	23

【源目 IP 一般都没问题，源目端口的确定理解为：谁发起协议连接的，那一行的目的 IP 就是协议端口号，即如第三、四行，功能是允许外部访问内部节点，因此需要调用 HTTP 协议目的端口是 80，这个请求是外部发起的，而外部连接进入的端口号不是熟知端口号>1023，因此源

端口号是>1023, 请求的发起人是外部, 因此在源 IP 那一行写上源端口是>1023 目的端口是 80, 同理可推第一、二行，总之即，源 IP 为协议发起者的那一行，目的端口是协议端口号，报文方向相反则源目端口号也颠倒】

第九章

R2.在视频中有两种类型的冗余。描述它们，并讨论如何能够利用它们进行有效压缩。

答：①空间冗余——给定图像内的冗余。从直观上看，一幅主要由空白构成的图像具有高度的冗余，可以在不显著牺牲图像质量的情况下进行有效压缩。②时间冗余——反映了从图像到后续图像的重复。例如，如果一幅图像与后续图像完全相同，则没有理由对后续图像进行重新编码；相反，在编码期间简单地指出后续图像完全相同会更有效。如果两幅图像非常相似，则可能无法有效地指出第二幅图像与第一幅图像的区别，而不是重新编码第二幅图像。

R3.假定一个模拟音频信号每秒抽样 16000 次，并且每个样本量化为 1024 级之一，该 PCM 数字音频信号的比特率将是多少？

答：将一个样本量化为 1024 级意味着每个样本有 10 位。PCM 数字音频信号的最终速率是 160kbps。

R4.多媒体应用能够分为三种类型。阐述它们的名称并对每种类型进行描述。

答：　①流媒体存储音频/视频——在这类应用程序中，底层媒体是预先录制的视频，例如电影、电视节目或预先录制的体育赛事。这些预先录制的视频将在服务器上播放，用户向服务器发送请求以按需观看视频。如今，许多互联网公司都提供流媒体视频，包括 YouTube、Netflix 和 Hulu。【优酷、人人视频】

②会话语音和 IP 上的视频——Internet 上的实时会话语音通常被称为 Internet 电话，因为从用户的角度来看，它类似于传统的电路交换电话服务。它也通常被称为 ip 语音(VOIP)。对话视频类似，除了它包括参与者的视频和他们的声音。会话语音和视频在今天的互联网上得到了广泛的应用，像 Skype 和谷歌 Talk 这样的互联网公司拥有数以亿计的日常用户。【微信语音/视频聊天、腾讯会议】

③流媒体实况音频/视频——这些应用程序允许用户通过互联网接收现场广播或电视传输。今天，世界各地成千上万的电台和电视台正在通过互联网广播内容。【虎牙直播、一直播】

R5.流式多媒体系统能够分为三种类型。阐述它们的名称并对每种类型进行描述。

答：　①UDP 流——有了 UDP 流，服务器传输视频的速率匹配客户的视频消费速率通过在 UDP 上以稳定的速率计时出视频块。【主要用于保证实时性，一般应用于视频会议这类软件】

②HTTP 流媒体——在 HTTP 流媒体，视频只是存储在一个 HTTP 服务器作为普通文件与一个特定的 URL。当用户想要查看视频时，客户端与服务器建立一个 TCP 连接，并针对该 URL 发出一个 HTTP GET 请求。然后服务器在 HTTP 响应消息中以尽可能快的速度发送视频文件，也就是说，以 TCP 拥塞控制和流控制允许的速度发送视频文件。【主要是可以避免被防火墙拦截，用于保证可靠性，一般应用于视频播放、缓存这类软件】

③自适应 HTTP 流(DASH)——在 HTTP 上的动态自适应流，视频被编码几个不同的版本，每个版本有一个不同的比特率，相应的，一个不同的质量水平。客户端动态地请求不同版本的几秒钟长的视频片段块。当可用带宽量高时，客户端自然地从高速率版本中选择块;当可用带宽很低时，它会自然地从低速率版本中选择。【P98，相当于在 HTTP 流的基础上提供自动适应当前网络环境来发送合适清晰度视频的功能】

R6.列举 UDP 流的三种缺点。

答：1. 由于服务器和客户端之间不可预测和变化的可用带宽量，恒定速率 UDP 流可能无法提供连续播放。2. 它需要一个媒体控制服务器(例如 RTSP 服务器)来处理客户机到服务器的交互请求，并跟踪每个正在进行的客户机会话的客户机状态。3. 许多防火墙被配置为阻止 UDP 通信，这会阻止在防火墙后的用户接收到 UDP 视频。【第二点中，所谓“客户到服务器的交互请求”比如暂停、播放、同步客户端播放点】

R7.对于 HTTP 流，TCP 接收缓存和客户应用缓存是相同的东西吗？如果不是，它们是怎样交互的呢？
答：不是。在客户端，客户端应用程序从 TCP 接收缓存读取字节，并将这些字节放在客户端应用程序缓存中。【TCP 接收缓存中的东西类型很多，不止包括应用缓存的内容】

R8.考虑对于 HTTP 流的简单模型。假设服务器以 2Mbps 的恒定速率发送比特，并且当已经接收到 800 万比特时开始播放。初始缓存时延 t_p 是多少？
答：初始缓冲延迟为 $t_p = Q/x = 4$ 秒。

R9.端到端时延和分组时延抖动的区别是什么？分组时延抖动的原因是什么？
答：端到端时延是数据包通过网络从源到目的地的时间。延时抖动是指数据包到下一个数据包的端到端延迟的波动。【前者是样本，后者是样本之间的差值，表示实际情况之间的波动状况】

R10.为什么在预定的播放时间之后收到的分组被认为是丢失了？
答：在预定的播放时间之后到达的数据包不能播放。因此，从应用程序的角度来看，数据包已经丢失了。

R11.总结两种 FEC 方案。这两种方案通过增加开销而增加了流的传输速率。交织技术也会增加传输速率吗？
答：　　第一个方案——每 n 个块后发送一个冗余编码块；通过对 n 个原始块进行异或运算得到冗余块。
　　第二种方案——与原始流发送一个低分辨率低比特率方案。
　　交织不会增加流的带宽要求。

P1.【P473】
答：　　a. 客户就开始播出第一块到达 t1 和视频块要在固定的时间 d。所以接下来的是第二段视频块，它应该到达时间 $t_1 + d$ 是在正确的时间,第三块 $t_1 + 2d$ 等等。从图中我们可以看到，只有编号为 1、4、5、6 的块在它们的播放时间之前到达接收器。
　　b. 客户开始播出时间 $t_1 + d$ 和视频块要在固定的时间 d。所以接下来的是第二段视频块，它应该到达时间 $t_1 + 2d$ 是在正确的时间，第三块 $t_1 + 3d$ 等等。从图中可以看出，除了 7 个之外，从 1 到 6 个视频块在播放时间之前到达接收器。
　　c. 在客户端缓冲区中最多存储两个视频块。分别为 3 和 4 的视频块在 $t_1 + 3d$ 之前和 $t_1 + 2d$ 之后到达，因此将这两个视频块存储在客户端缓冲区中。编号为 5 的视频块在时间 $t_1 + 4d$ 之前和 $t_1 + 3d$ 之后到达，与编号为 4 的已存储视频块一起存储在客户端缓冲区中。
　　d. 在客户处最小的播放时延应该是 $t_1 + 3d$，以确保每个区块都能及时到达。
【答题时在横坐标上标号，此时正在播放第 n 帧，在折线上标号，这是第几个帧，一目了然。播放时延就是第一个块到达后，等待一个播放时延再开始播放（可以理解为等播放器缓冲多长时间）】

P11.【P475】
答：　　a. 分组 2 的时延是 7 个时隙。分组 3 的时延是 9 个时隙。分组 4 的时延是 8 个时隙。分组 5 的时延是 7 个时隙。分组 6 的时延是 9 个时隙。分组 7 的时延是 8 个时隙。分组 8 的时延是>8 时隙。【所谓分组的时延就是发送方发出到接收方播放之间的时延，该题忽略播放时延】
　　b.3、4、6、7、8 均不能按时到。
　　c.3、6 不能按时到。

d.10。

P16.是非判断：

a.如果存储视频直接从 Web 服务器流式传输到媒体播放器，这个应用则正在使用 TCP 作为底层的传输协议。

答：正确。

b.当使用 RTP 时，发送方有可能在会话中改变编码。

答：正确。

c.所有使用 RTP 的应用必须使用端口 87.

答：错误。RTP 流可以发送到/从任何端口号。请参阅第 9.4 节中的 SIP 示例。

d.假设一个 RTP 会话对每个发送方有独立的音频和视频流，则这些音频和视频流使用同样的 SSRC。

答：错误。他们通常被赋予不同的 SSRC 值。

e.在区分服务中，尽管每跳行为定义了各类型之间的性能差别，但它没有强制要求为了获得这些性能而使用任何特定机制。

答：正确。

f.假设 Alice 要和 Bob 建立一个 SIP 会话。在她的 INVITE 报文中包括了这样的行：m=audio 48753 RTP/AVP 3（AVP3 指示 GSM 音频）。因此 Alice 在该报文中指示她要发送 GSM 音频。

答：错误。她表明她希望接收 GSM 音频。

g.仍是上一句的行。Alice 在她的 INVITE 报文中指示了她将把音频发送到端口 48753。

答：错误。她表明她希望通过该端口接收音频。

h.SIP 报文在 SIP 实体之间通常使用一个默认的 SIP 端口号发送。

答：正确。源端口号和目标端口号均为 5060。

i.为了维护注册，SIP 客户必须周期地发送 REGISTER 报文。

答：正确。

j.SIP 强制所有的 SIP 客户支持 G.711 音频编码。

答：错误。这是 H.323 的要求。

P17.【P476】

答：a.

Time Slot	Packets in the queue	Number of tokens in bucket
0	1, 2, 3	2
1	3, 4	1
2	4,5	1
3	5,6	1
4	6	1
5	-	1
6	7, 8	2
7	9, 10	1
8	10	1

b.

Time Slot	Packets in output buffer
0	1, 2
1	3
2	4
3	5
4	6
5	-
6	7, 8
7	9
8	10