练习题答案

第 1 章

1. 计算机网络都有哪些类别？各种类别的网络有哪些特点？

答：按范围：(1) 广域网 WAN：远程、高速，是 Internet 的核心网。

(2) 城域网：城市范围，连接多个局域网。

(3) 局域网：校园、企业、机关、社区。

(4) 个域网 PAN：个人电子设备。

按用户：公用网：面向公共营运。专用网：面向特定机构。

2. 因特网的两大组成部分（边缘部分与核心部分）的特点是什么？它们的工作方式各有什么特点？

答：边缘部分：由各主机构成，用户直接进行信息处理和信息共享；低速连入核心网。核心部分：由各路由器连网，负责为边缘部分提供高速远程分组交换。

3. 客户—服务器方式与对等方式的主要区别是什么？有没有相同的地方？

答：前者严格区分服务和被服务者，后者无此区别。后者实际上是前者的双向应用。

4. 计算机网络有哪些常用的性能指标？

答：速率，带宽，吞吐量，时延，时延带宽积，往返时间 RTT，利用率。

5. 论述具有五层协议的网络体系结构的要点，包括各层的主要功能。

答：综合 OSI 参考模型和 TCP/IP 参考模型的优点，采用一种原理体系结构。各层的主要功能：物理层的任务就是透明地传送比特流。（注意：传递信息的物理媒体，如双绞线、同轴电缆、光缆等，是在物理层的下面，当作第 0 层。）物理层还要确定连接电缆插头的定义及连接法。数据链路层的任务是在两个相邻节点间的线路上无差错地传送以帧（frame）为单位的数据，每一帧包括数据和必要的控制信息。网络层的任务是选择合适的路由，使发送站的传输层所传下来的分组能够正确无误地按照地址找到目的站，并交付给目的站的传输层。传输层的任务是向上一层的进行通信的两个进程之间提供一个可靠的端到端服务，使它们看不见传输层以下的数据通信的细节。应用层直接为用户的应用进程提供服务。

第 2 章

1. 物理层要解决哪些问题？物理层的主要特点是什么？

答：(1) 物理层要尽可能地屏蔽掉物理设备和传输媒体，通信手段的不同使数据链路

层感觉不到这些差异，只考虑完成本层的协议和服务。(2) 给其服务用户（数据链路层）在一条物理的传输媒体上传送和接收比特流（一般为串行按顺序传输的比特流）的能力，为此，物理层应该解决物理连接的建立、维持和释放问题。(3) 在两个相邻系统之间唯一地标识数据电路。

物理层的主要特点：(1) 由于在 OSI 参考模型之前，许多物理规程或协议已经制定出来了，而且在数据通信领域中，这些物理规程已被许多商品化的设备所采用，加之物理层协议涉及的范围广泛，所以至今没有按 OSI 参考模型制定一套新的物理层协议，而是沿用已存在的物理规程，将物理层确定为描述与传输媒体接口的机械、电气、功能和规程特性。(2) 由于物理连接的方式很多，传输媒体的种类也很多，因此，具体的物理协议相当复杂。

2. 物理层的接口有哪几个方面的特性？各包含什么内容？

答：(1) 机械特性，明接口所用的接线器的形状和尺寸、引线数目和排列、固定和锁定装置等。(2) 电气特性，指明在接口电缆的各条线上出现的电压的范围。(3) 功能特性，指明某条线上出现的某一电平的电压表示何意。(4) 规程特性，说明对于不同功能的各种可能事件的出现顺序。

3. 常用的传输介质有哪几种？各有何特点？

答：双绞线有屏蔽双绞线 STP（shielded twisted pair）、无屏蔽双绞线 UTP（unshielded twisted pair），同轴电缆有 50 Ω 同轴电缆、75 Ω 同轴电缆。

光纤有单模光纤和多模光纤。

无线传输有短波通信、微波、卫星通信。

4. 为什么要使用信道复用技术？常用的信道复用技术有哪些？

答：为了通过共享信道、最大限度提高信道利用率。

常用的信道复用技术频分、时分、码分、波分复用技术。

5. 共有四个站进行码分多址 CDMA 通信。四个站的码片序列为：

A：(−1−1−1+1+1−1+1+1)　　***B***：(−1−1+1−1+1+1+1−1)

C：(−1+1−1+1+1+1−1−1)　　***D***：(−1+1−1−1−1−1+1−1)

现收到这样的码片序列 ***S***：(−1+1−3+1−1−3+1+1)。试问哪个站发送数据了？发送数据的站发送的是 1 还是 0？

解：$\boldsymbol{S}\cdot\boldsymbol{A}=(+1-1+3+1-1+3+1+1)/8=1$，A 发送 1。

$\boldsymbol{S}\cdot\boldsymbol{B}=(+1-1-3-1-1-3+1-1)/8=-1$，B 发送 0。

$\boldsymbol{S}\cdot\boldsymbol{C}=(+1+1+3+1-1-3-1-1)/8=0$，C 无发送。

$\boldsymbol{S}\cdot\boldsymbol{D}=(+1+1+3-1+1+3+1-1)/8=1$，D 发送 1。

第 3 章

1. 数据链路（即逻辑链路）与链路（即物理链路）有何区别？“电路接通了”与“数据链路接通了”有何区别？

答：数据链路与链路的区别在于数据链路除链路外，还必须有一些必要的规程来控制

数据的传输，因此，数据链路比链路多了实现通信规程所需要的硬件和软件。“电路接通了”表示链路两端的节点交换机已经开机，物理连接已经能够传送比特流了，但是，数据传输并不可靠，在物理连接基础上，再建立数据链路连接，才是“数据链路接通了”，此后，由于数据链路连接具有检测、确认和重传功能，才使不太可靠的物理链路变成可靠的数据链路，进行可靠的数据传输。当数据链路断开连接时，物理连接不一定跟着断开连接。

2. 网桥的工作原理和特点是什么？网桥与以太网交换机有何异同？

答：网桥工作在数据链路层，它根据 MAC 帧的目的地址对收到的帧进行转发。网桥具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的接口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定将该帧转发到哪一个接口转发器工作在物理层，它仅简单地转发信号，没有过滤能力以太网交换机则为数据链路层设备，可视为多端口网桥。

3. 网络适配器的作用是什么？网络适配器工作在哪一层？

答：适配器（即网卡）来实现数据链路层和物理层这两层的协议的硬件和软件网络适配器工作在 TCP/IP 模型的网络接口层（OSI 模型的数据链里层和物理层）。

4. 要发送的数据为 1101011011。采用 CRC 的生成多项式是 $P(x)=x^4+x+1$。试求应添加在数据后面的余数。若要发送的数据在传输过程中最后一个 1 变成了 0，问接收端能否发现？若要发送的数据在传输过程中最后两个 1 都变成了 0，问接收端能否发现？采用 CRC 检验后，数据链路层的传输是否就变成了可靠的传输？

答：作二进制除法，11010110110000 除以 10011，余数 1110，添加的检验序列是 1110。

作二进制除法，余数都不为 0，两种错误均可发现。

仅仅采用了 CRC 检验，缺重传机制，数据链路层的传输还不是可靠的传输。

5. 要发送的数据为 101110。采用 CRC 的生成多项式是 $P(x)=x^3+1$。试求应添加在数据后面的余数？

答：作二进制除法，101110000 除以 10011，余数为 011，添加在数据后面的余数是 011。

6. 如图 3-21 所示，以太网交换机有 6 个接口，分别连接 5 台主机和一个路由器。

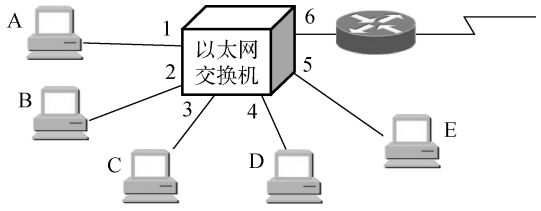

图 3-21　习题 6 的图

在下表的“动作”一栏中，表示先后发送了 4 个帧。假定在开始时，以太网交换机的交换表是空的，试把该表中其他的栏目都填写完。

动作	交换表的状态	向哪些接口转发帧	说明
A 发送帧给 D	写入（A，1）	向除 1 以外的所有接口广播	略
D 发送帧给 A	写入（D，4）	向 1 接口转发帧	略
E 发送帧给 A	写入（E，1）	向 1 接口转发帧	略
A 发送帧给 E	不变	向 5 接口转发帧	略

第 4 章

1. 什么是局域网？局域网的主要特点是什么？

答：局域网 LAN 是指在较小的地理范围内，将有限的通信设备互联起来的计算机通信网络。从功能的角度来看，局域网具有以下几个特点：（1）共享传输信道，在局域网中，多个系统连接到一个共享的通信媒体上。（2）地理范围有限，用户个数有限。通常局域网仅为一个单位服务，只在一个相对独立的局部范围内连网，如一座楼或集中的建筑群内。一般来说，局域网的覆盖范围为 10 m～10 km 或更大一些。

2. 什么是介质访问控制方法？常用的介质访问控制方法有哪几种？

答：介质访问控制方法的主要内容有两个方面：一是要确定网络上每一个节点能够将信息发送到介质上去的特定时刻，二是要解决如何对共享介质访问和利用加以控制。常用的介质访问控制方法有 3 种：总线结构的带冲突检测的载波监听多路访问 CSMA/CD 方法、环形结构的令牌环（token ring）访问控制方法和令牌总线（token bus）访问控制方法。

3. 什么是 CSMA/CD？简述其特点和基本工作原理。

答：CSMA/CD（carrier sense multiple access/collision detection）采用的是争用技术的一种介质访问控制方法，中文名是带有冲突检测的载波侦听多路访问。工作原理：发送前先监听，边发送边监听，一旦发现总线上出现了碰撞，就立即停止发送。然后按照退避算法等待一段随机时间后再次发送。因此，每一个站在自己发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。

4. 什么是 VLAN？有哪些方法可以实现 VLAN？请简述各种方法的特点。

答：VLAN 是虚拟局域网，VLAN 的实现方式包括静态 VLAN 和动态 VLAN 两种。静态 VLAN 由网络管理员根据交换机端口进行静态的 VALN 分配，当在交换机上把其某一个端口分配给一个 VLAN 时，将一直保持不变直到网络管理员改变这种配置，所以又被称为基于端口的 VLAN。动态 VLAN 是指交换机上以联网用户的 MAC 地址、逻辑地址（如 IP 地址）或数据报协议等信息为基础将交换机端口动态分配给 VLAN 的方式。当用户的主机连入交换机端口时，交换机通过检查 VLAN 管理数据库中相应的关于 MAC 地址、逻辑地址（如 IP 地址）或数据报协议的表项，以相应的数据库表项内容动态地配置相应的交换机端口。

5. 试说明 10 Base－T 中的“10”“BASE”和“T”所代表的意思。

答：10 Base－T 中的“10”表示信号在电缆上的传输速率为 10 Mbps，“BASE”表示

电缆上的信号是基带信号，“T”代表双绞线星型网，但 10 Base－T 的通信距离稍短，每个站到集线器的距离不超过 100 m。

6. 有 10 个站连接到以太网上。试计算以下三种情况下每一个站所能得到的带宽。

（1）10 个站都连接到一个 10 Mbps 以太网集线器。

（2）10 个站都连接到一个 100 Mbps 以太网集线器。

（3）10 个站都连接到一个 10 Mbps 以太网交换机。

答：（1）10 个站都连接到一个 10 Mbps 以太网集线器：10 个站共享 10 Mbps。

（2）10 个站都连接到一个 100 Mbps 以太网集线器：10 个站共享 100 Mbps。

（3）10 个站都连接到一个 10 Mbps 以太网交换机：每个站独占 10 Mbps。

第 5 章

1. 网络层向上提供的服务有哪两种？试比较其优缺点。

答：网络层向传输层提供“面向连接”虚电路（virtual circuit）服务或“无连接”数据报服务前者预约了双方通信所需的一切网络资源。前者的优点是能提供服务质量的承诺，即所传送的分组不出错、丢失、重复和失序（不按序列到达终点），也保证分组传送的时限，缺点是路由器复杂，网络成本高；后者无网络资源障碍，尽力而为，优缺点与前者互易。

2. 作为中间设备，转发器、网桥、路由器和网关有何区别？

答：中间设备又称为中间系统或中继（relay）系统。

物理层中继系统：转发器（repeater）。

数据链路层中继系统：网桥或桥接器（bridge）。

网络层中继系统：路由器（router）。

网桥和路由器的混合物：桥路器（brouter）。

网络层以上的中继系统：网关（gateway）。

3. 试简单说明下列协议的作用：IP、ARP、RARP 和 ICMP。

答：IP：实现网络互联。使参与互联的性能各异的网络从用户看起来好像是一个统一的网络。互联网协议 IP 是 TCP/IP 体系中两个最主要的协议之一，与 IP 配套使用的还有四个协议。

ARP：是解决同一个局域网上的主机或路由器的 IP 地址和硬件地址的映射问题。

RARP：是解决同一个局域网上的主机或路由器的硬件地址和 IP 地址的映射问题。

ICMP：提供差错报告和询问报文，以提高 IP 数据交付成功的机会。

因特网组管理协议 IGMP：用于探寻、转发本局域网内的组成员关系。

4. IP 地址分为几类？分别如何表示？IP 地址的主要特点是什么？

答：分为 A、B、C、D、E5 类。

每一类地址都由两个固定长度的字段组成，其中一个字段是网络号 net－id，它标志主机（或路由器）所连接到的网络；另一个字段则是主机号 host－id，它标志该主机（或路由器）。各类地址的网络号字段 net－id 分别为 1 字节、2 字节、3 字节、0 字节、0 字

节；主机号字段 host－id 分别为 3 字节、2 字节、1 字节、4 字节、4 字节。

特点：（1）IP 地址是一种分等级的地址结构。分两个等级的好处：第一，IP 地址管理机构在分配 IP 地址时只分配网络号，而剩下的主机号则由得到该网络号的单位自行分配。这样就方便了 IP 地址的管理。第二，路由器仅根据目的主机所连接的网络号来转发分组（而不考虑目的主机号），这样就可以使路由表中的项目数大幅度减少，从而减小了路由表所占的存储空间。（2）实际上 IP 地址是标志一个主机（或路由器）和一条链路的接口。当一个主机同时连接到两个网络上时，该主机就必须同时具有两个相应的 IP 地址，其网络号 net－id 必须是不同的。这种主机称为多归属主机（multihomed host）。由于一个路由器至少应当连接到两个网络（这样它才能将 IP 数据报从一个网络转发到另一个网络），因此一个路由器至少应当有两个不同的 IP 地址。（3）用转发器或网桥连接起来的若干个局域网仍为一个网络，因此这些局域网都具有同样的网络号 net－id。（4）所有分配到网络号 net－id 的网络，范围很小的局域网，还是可能覆盖很大地理范围的广域网，都是平等的。

5. 试说明 IP 地址与硬件地址的区别，以及为什么要使用这两种不同的地址？

答：IP 地址就是给每个连接在因特网上的主机（或路由器）分配一个在全世界范围是唯一的 32 位的标识符，从而把整个因特网看成为一个单一的、抽象的网络在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。

硬件地址在一定程度上与硬件一致，基于物理、能够标识具体的链路通信对象、IP 地址给予逻辑域的划分、不受硬件限制。

6. 子网掩码为 255.255.255.0 代表什么意思？

答：有三种含义：

其一是一个 A 类网的子网掩码，对于 A 类网络的 IP 地址，前 8 位表示网络号，后 24 位表示主机号，使用子网掩码 255.255.255.0 表示前 8 位为网络号，中间 16 位用于子网段的划分，最后 8 位为主机号。

其二是一个 B 类网，对于 B 类网络的 IP 地址，前 16 位表示网络号，后 16 位表示主机号，使用子网掩码 255.255.255.0 表示前 16 位为网络号，中间 8 位用于子网段的划分，最后 8 位为主机号。

其三是一个 C 类网，这个子网掩码为 C 类网的默认子网掩码。

7. 网络子网掩码为 255.255.255.248，问该网络能够连接多少个主机？

答：255.255.255.248 即 11111111.11111111.11111111.11111000，每一个子网上的主机为 $2^3-2=6$ 台。

子网掩码位数为 29，该网络能够连接 8 个主机，扣除全 1 和全 0 后为 6 台。

8. A 类网络和 B 类网络的子网号分别为 16 个 1 和 8 个 1，问这两个网络的子网掩码有何不同？

答：A 类网络：11111111　11111111　11111111　00000000。给定子网号（16 位“1”），则子网掩码为 255.255.255.0。

B 类网络：11111111　11111111　11111111　00000000。给定子网号（8 位“1”），则子网掩码为 255.255.255.0，但子网数目不同。

9. 一个 B 类地址的子网掩码是 255.255.240.0。试问在其中每一个子网上的主机数最多是多少？

答：$(240)_{10}=(128+64+32+16)_{10}=(11110000)_2$

Host－id 的位数为 4＋8＝12，因此，最大主机数为：$2^{12}-2=4096-2=4094$ 台。

10. A 类网络的子网掩码为 255.255.0.255，它是否为一个有效的子网掩码？

答：是。

11. C 类网络使用子网掩码有无实际意义？为什么？

答：有实际意义。C 类子网 IP 地址的 32 位中，前 24 位用于确定网络号，后 8 位用于确定主机号。如果划分子网，可以选择后 8 位中的高位，这样做可以进一步划分网络，并且不增加路由表的内容，但是代价是主机数相信减少。

12. 试辨认以下 IP 地址的网络类别。

(1) 128.36.199.3。

(2) 21.12.240.17。

(3) 183.194.76.253。

(4) 192.12.69.248。

(5) 89.3.0.1。

(6) 200.3.6.2。

答：(2) 和 (5) 是 A 类，(1) 和 (3) 是 B 类，(4) 和 (6) 是 C 类。

13. 一个 3200 位长的 TCP 报文传到 IP 层，加上 160 位的首部后成为数据报。下面的互联网由两个局域网通过路由器连接起来。但第二个局域网所能传送的最长数据帧中的数据部分只有 1200 位。因此数据报在路由器必须进行分片。试问第二个局域网向其上层要传送多少位数据（这里的“数据”指的是局域网看见的数据）？

答：第二个局域网所能传送的最长数据帧中的数据部分只有 1200 bit，即每个 IP 数据片的数据部分＜1200－160 (bit)，由于片偏移是以 8 字节即 64 bit 为单位的，所以 IP 数据片的数据部分最大不超过 1024 bit，这样 3200 bit 的报文要分 4 个数据片，所以第二个局域网向上传送的位数等于 (3200＋4×160)，共 3840 bit。

14. 设某路由器建立了如下路由表。

目的网络	子网掩码	下一跳
128.96.39.0	255.255.255.128	接口 m0
128.96.39.128	255.255.255.128	接口 m1
128.96.40.0	255.255.255.128	R2
192.4.153.0	255.255.255.192	R3
＊（默认）	——	R4

现共收到 5 个分组，其目的地址分别为：

(1) 128.96.39.10。

(2) 128.96.40.12。

(3) 128.96.40.151。

(4) 192.153.17。

(5) 192.4.153.90。

试分别计算下一跳。

答：(1) 分组的目的站 IP 地址为 128.96.39.10，与子网掩码 255.255.255.128 相与得 128.96.39.0，可见该分组经接口 0 转发。

(2) 分组的目的 IP 地址为 128.96.40.12。

①与子网掩码 255.255.255.128 相与得 128.96.40.0，不等于 128.96.39.0。

②与子网掩码 255.255.255.128 相与得 128.96.40.0，经查路由表可知，该项分组经 R2 转发。

(3) 分组的目的 IP 地址为 128.96.40.151，与子网掩码 255.255.255.128 相与后得 128.96.40.128，与子网掩码 255.255.255.192 相与后得 128.96.40.128，经查路由表知，该分组转发选择默认路由，经 R4 转发。

(4) 分组的目的 IP 地址为 192.4.153.17，与子网掩码 255.255.255.128 相与后得 192.4.153.0，与子网掩码 255.255.255.192 相与后得 192.4.153.0，经查路由表知，该分组经 R3 转发。

(5) 分组的目的 IP 地址为 192.4.153.90，与子网掩码 255.255.255.128 相与后得 192.4.153.0，与子网掩码 255.255.255.192 相与后得 192.4.153.64，经查路由表知，该分组转发选择默认路由，经 R4 转发。

15. 一个数据报长度为 4000 字节（固定首部长度）。现在经过一个网络传送，但此网络能够传送的最大数据长度为 1500 字节。试问应当划分为几个短些的数据报片？各数据报片的数据字段长度、片偏移字段和 MF 标志应为何数值？

答：IP 数据报固定首部长度为 20 字节

总长度（字节）	数据长度（字节）	MF	片偏移
原始数据报	4000	3980	0	0
数据报片 1	1500	1480	1	0
数据报片 2	1500	1480	1	185
数据报片 3	1040	1020	0	370

16. 试找出可产生以下数目的 A 类子网的子网掩码（采用连续掩码）。

(1) 2。(2) 6。(3) 30。(4) 62。(5) 122。(6) 250。

答：(1) 255.192.0.0。(2) 255.224.0.0。(3) 255.248.0.0。(4) 255.252.0.0。(5) 255.254.0.0。(6) 255.255.0.0。

17. 与下列掩码相对应的网络前缀各有多少位？

(1) 192.0.0.0。(2) 240.0.0.0。(3) 255.254.0.0。(4) 255.255.255.252。

答：(1) /2 。(2) /4。(3) /11。(4) /30。

18. 已知地址块中的一个地址是 140.120.84.24/20。试问：这个地址块中的最小地址和最大地址各为多少？地址掩码是什么？地址块中共有多少个地址？相当于多少个 C 类地址？

答：140.120.84.24 可写成 140.120.（0101 0100）.24。

最小地址是 140.120.（0101 0000）.0/20（80）。

最大地址是 140.120.（0101 1111）.255/20（95）。

地址数是 4096 个，相当于 16 个 C 类地址。

19. 假定网络中的路由器 B 的路由表有如下项目（这三列分别表示“目的网络”、“距离”和“下一跳路由器”）：

N1　7　A
N2　2　B
N6　8　F
N8　4　E
N9　4　F

现在 B 收到从 C 发来的路由信息（这两列分别表示“目的网络”“距离”）：

N2　4
N3　8
N6　4
N8　3
N9　5

试求出路由器 B 更新后的路由表（详细说明每一个步骤）。

答：路由器 B 更新后的路由表如下：

N1　7　A　无新信息，不改变
N2　5　C　相同的下一跳，更新
N3　9　C　新的项目，添加进来
N6　5　C　不同的下一跳，距离更短，更新
N8　4　E　不同的下一跳，距离一样，不改变
N9　4　F　不同的下一跳，距离更大，不改变

20. 假定网络中的路由器 A 的路由表有如下的项目（格式同上题）：

N1　4　B
N2　2　C
N3　1　F
N4　5　G

现将 A 收到从 C 发来的路由信息（格式同上题）：

N1　2
N2　1
N3　3
N4　7

试求出路由器 A 更新后的路由表（详细说明每一个步骤）。

答：路由器 A 更新后的路由表如下：

N1　3　C　不同的下一跳，距离更短，改变
N2　2　C　不同的下一跳，距离一样，不变
N3　1　F　不同的下一跳，距离更大，不改变
N4　5　G　无新信息，不改变

21. 某单位分配到一个起始地址为 14.24.74.0/24 的地址块。该单位需要用到 3 个子网，他们的 3 个子地址块的具体要求为：子网 N_1 需要 120 个地址，子网 N_2 需要 60 个地址，子网 N_3 需要 10 个地址。请给出地址块的分配方案。

答：分配给子网 N_1 的首地址是 14.24.74.0/25，末地址是 14.24.74.127/25。

分配给子网 N_2 的首地址是 14.24.74.128/26，末地址是 14.24.74.191/26。

分配给子网 N_3 的首地址是 14.24.74.192/28，末地址是 14.24.74.207/28。

第 6 章

1. 试说明传输层在协议栈中的地位和作用。传输层的通信和网络层的通信有什么重要的区别？为什么传输层是必不可少的？

答：传输层处于面向通信部分的最高层，同时也是用户功能中的最低层，向它上面的应用层提供服务运输层为应用进程之间提供端到端的逻辑通信，但网络层是为主机之间提供逻辑通信（面向主机，承担路由功能，即主机寻址及有效的分组交换）。各种应用进程之间通信需要“可靠或尽力而为”的两类服务质量，必须由传输层以复用和分用的形式加载到网络层。

2. 接收方收到有差错的 UDP 用户数据报时应如何处理？

答：丢弃。

3. 如果应用程序愿意使用 UDP 完成可靠传输，这可能吗？请说明理由。

答：可能，但应用程序中必须额外提供与 TCP 相同的功能。

4. 为什么说 UDP 是面向报文的，而 TCP 是面向字节流的？

答：发送方 UDP 对应用程序交下来的报文，在添加首部后就向下交付 IP 层。UDP 对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。接收方 UDP 对 IP 层交上来的 UDP 用户数据报，在去除首部后就原封不动地交付上层的应用进程，一次交付一个完整的报文。发送方 TCP 对应用程序交下来的报文数据块，视为无结构的字节流。

5. 端口的作用是什么？为什么端口号要划分为 3 种？

答：端口的作用是对 TCP/IP 体系的应用进程进行统一的标志，使运行不同操作系统的计算机的应用进程能够互相通信。保留端口一般都小于 1024，它们基本上都被分配给了已知的应用协议；动态分配的端口一般都大于 1024，这一类的端口没有固定的使用者，它们可以被动态地分配给应用程序使用；注册端口比较特殊，也是固定为某个应用服务的端口，但是它所代表的不是已经形成标准的应用层协议，而是某个软件厂商开发的应用程序。

6. 某个应用进程使用传输层的用户数据报 UDP，然后继续向下交给 IP 层后，又封装成 IP 数据报。既然都是数据报，是否可以跳过 UDP 而直接交给 IP 层？哪些功能 UDP 提供了但 IP 没有提供？

答：不可跳过 UDP 而直接交给 IP 层 IP 数据报 IP 报承担主机寻址，提供报头检错；只能找到目的主机而无法找到目的进程。UDP 提供对应用进程的复用和分用功能，以及提供对数据差分的差错检验。

7. 主机 A 向主机 B 连续发送了两个 TCP 报文段，其序号分别为 70 和 100。试问：

（1）第一个报文段携带了多少个字节的数据？

（2）主机 B 收到第一个报文段后发回的确认中的确认号应当是多少？

（3）如果主机 B 收到第二个报文段后发回的确认中的确认号是 180，试问主机 A 发送

的第二个报文段中的数据有多少字节？

（4）如果主机 A 发送的第一个报文段丢失了，但第二个报文段到达了主机 B。主机 B 在第二个报文段到达后向主机 A 发送确认。试问这个确认号应为多少？

答：（1）第一个报文段的数据序号是 70 到 99，共 30 字节的数据。

（2）确认号应为 100。

（3）80 字节。

（4）70。

8. 在 TCP 的拥塞控制中，什么是慢开始、拥塞避免、快重传和快恢复算法？每一种算法各起什么作用？“乘法减小”和“加法增大”各用在什么情况下？

答：慢开始：在主机刚刚开始发送报文段时可先将拥塞窗口 cwnd 设置为一个最大报文段 MSS 的数值。在每收到一个对新的报文段的确认后，将拥塞窗口增加至多一个 MSS 的数值。用这样的方法逐步增大发送端的拥塞窗口 cwnd，可以分组注入到网络的速率更加合理。

拥塞避免：当拥塞窗口值大于慢开始门限时，停止使用慢开始算法而改用拥塞避免算法。拥塞避免算法使发送的拥塞窗口每经过一个往返时延 RTT 就增加一个 MSS 的大小。

快重传算法：发送端只要一连收到 3 个重复的 ACK 即可断定有分组丢失了，就应该立即重传丢失的报文段而不必继续等待为该报文段设置的重传计时器的超时。

快恢复算法：当发送端收到连续 3 个重复的 ACK 时，就重新设置慢开始门限 ssthresh 与慢开始不同之处是拥塞窗口 cwnd 不是设置为 1，而是设置为 ssthresh 若收到的重复的 AVK 为 n 个（$n>3$），则将 cwnd 设置为 ssthresh 若发送窗口值还容许发送报文段，就按拥塞避免算法继续发送报文段。若收到了确认新的报文段的 ACK，就将 cwnd 缩小到 ssthresh。

乘法减小：是指不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一次网络拥塞），就把慢开始门限值 ssthresh 设置为当前的拥塞窗口值乘以 0.5。当网络频繁出现拥塞时，ssthresh 值就下降得很快，以大大减少注入网络中的分组数。加法增大：是指执行拥塞避免算法后，在收到对所有报文段的确认后（即经过一个往返时间），就把拥塞窗口 cwnd 增加一个 MSS 大小，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

9. 设 TCP 的 ssthresh 的初始值为 8（单位为报文段）。当拥塞窗口上升到 12 时网络发生了超时，TCP 使用慢开始和拥塞避免。试分别求出第 1 次到第 15 次传输的各拥塞窗口大小。你能说明拥塞控制窗口每一次变化的原因吗？

答：拥塞窗口大小分别为 1、2、4、8、9、10、11、12、1、2、4、6、7、8、9。

10. TCP 的拥塞窗口 cwnd 大小与传输轮次 n 的关系如下表所示。

cwnd	1	2	4	8	16	32	33	34	35	36	37	38	39
n	1	2	3	4	5	6	7	8	9	10	11	12	13
cwnd	40	41	42	21	22	23	24	25	26	1	2	4	8
n	14	15	16	17	18	19	20	21	22	23	24	25	26

（1）试画出如图 6-14 所示的拥塞窗口与传输轮次的关系曲线。

（2）指明 TCP 工作在慢开始阶段的时间间隔。

（3）指明 TCP 工作在拥塞避免阶段的时间间隔。

（4）在第 16 轮次和第 22 轮次之后发送方是通过收到 3 个重复的确认还是通过超时检测到丢失了报文段？

（5）在第 1 轮次，第 18 轮次和第 24 轮次发送时，门限 ssthresh 分别被设置为多大？

（6）在第几轮次发送出第 70 个报文段？

（7）假定在第 26 轮次之后收到了 3 个重复的确认，因而检测出了报文段的丢失，那么拥塞窗口 cwnd 和门限 ssthresh 应设置为多大？

答：（1）略

（2）慢开始时间间隔：[1，6] 和 [23，26]。

（3）拥塞避免时间间隔：[6，16] 和 [17，22]。

（4）在第 16 轮次之后发送方通过收到 3 个重复的确认检测到丢失的报文段。在第 22 轮次之后发送方是通过超时检测到丢失的报文段。

（5）在第 1 轮次发送时，门限 ssthresh 被设置为 32 在第 18 轮次发送时，门限 ssthresh 被设置为发生拥塞时的一半，即 21. 在第 24 轮次发送时，门限 ssthresh 是第 18 轮次发送时设置的 21。

（6）第 70 报文段在第 7 轮次发送出。

（7）拥塞窗口 cwnd 和门限 ssthresh 应设置为 8 的一半，即 4。

第 7 章

1. 域名系统的主要功能是什么？域名系统中的本地域名服务器、根域名服务器、顶级域名服务器以及权限域名服务器有何区别？

答：域名系统的主要功能：将域名解析为主机能识别的 IP 地址。互联网上的域名服务器系统也是按照域名的层次来安排的。每一个域名服务器都只对域名体系中的一部分进行管辖。共有三种不同类型的域名服务器，即本地域名服务器、根域名服务器、授权域名服务器。当一个本地域名服务器不能立即回答某个主机的查询时，该本地域名服务器就以 DNS 客户的身份向某一个根域名服务器查询。若根域名服务器有被查询主机的信息，就发送 DNS 回答报文给本地域名服务器，然后本地域名服务器再回答发起查询的主机。但当根域名服务器没有被查询的主机的信息时，它一定知道某个保存有被查询的主机名字映射的授权域名服务器的 IP 地址。通常根域名服务器用来管辖顶级域。根域名服务器并不直接对顶级域下面所属的所有的域名进行转换，但它一定能够找到下面的所有二级域名的域名服务器。每一个主机都必须在授权域名服务器处注册登记。通常，一个主机的授权域名服务器就是它的主机 ISP 的一个域名服务器。授权域名服务器总是能够将其管辖的主机名转换为该主机的 IP 地址。互联网允许各个单位根据本单位的具体情况将本域名划分为若干个域名服务器管辖区。一般就在各管辖区中设置相应的授权域名服务器

2. 举例说明域名转换的过程。域名服务器中的高速缓存的作用是什么？

答：（1）把不方便记忆的 IP 地址转换为方便记忆的域名地址。

（2）作用：可大大减轻根域名服务器的负荷，使因特网上的 DNS 查询请求和回答报

文的数量大为减少。

3. 假设有一天整个互联网的 DNS 都瘫痪了（这种情况不太会出现），试问还有可能给朋友发送电子邮件吗？

答：不能

4. 简单文件传送协议 TFTP 与 FTP 的主要区别是什么？各用在什么场合？

答：文件传送协议 FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的运输服务。FTP 的主要功能是减少或消除在不同操作系统下处理文件的不兼容性。FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求；另外有若干个从属进程，负责处理单个请求。TFTP 是一个很小且易于实现的文件传送协议。TFTP 使用客户服务器方式和使用 UDP 数据报，因此 TFTP 需要有自己的差错改正措施 TFTP 只支持文件传输而不支持交互。TFTP 没有一个庞大的命令集，没有列目录的功能，也不能对用户进行身份鉴别。

5. 远程登录 telnet 的主要特点是什么？什么叫作虚拟终端 NVT？

答：（1）用户用 telnet 就可在其所在地通过 TCP 连接注册（即登录）到远地的另一个主机上（使用主机名或 IP 地址）。telnet 能将用户的击键传到远地主机，同时也能将远地主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。

（2）telnet 定义了数据和命令应该怎样通过因特网，这些定义就是所谓的网络虚拟终端 NVT。

6. 假定要从已知的 URL 获得一个万维网文档。若该万维网服务器的 IP 地址开始时并不知道。试问：除 HTTP 外，还需要什么应用层协议和传输层协议？

答：应用层协议需要的是 DNS。

运输层协议需要的是 UDP（DNS 使用）和 TCP（HTTP 使用）。

7. 试述电子邮件的最主要的组成部件。用户代理 UA 的作用是什么？没有 UA 行不行？

答：电子邮件系统的最主要组成部件：用户代理、邮件服务器以及电子邮件使用的协议。

UA 就是用户与电子邮件系统的接口。用户代理使用户能够通过一个很友好的接口来发送和接收邮件。没有 UA 不行。因为并非所有的计算机都能运行邮件服务器程序。有些计算机可能没有足够的存储器来运行允许程序在后台运行的操作系统，或是可能没有足够的 CPU 能力来运行邮件服务器程序。更重要的是，邮件服务器程序必须不间断地运行，每天 24 小时都必须不间断地连接在因特网上，否则就可能使很多外面发来的邮件丢失。这样看来，让用户的 PC 机运行邮件服务器程序显然是很不现实的。

第 8 章

1. 什么是网络安全？

答：网络安全从其本质上来讲就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠、正常地运行，网络服务不中断。

2. 计算机网络上的通信面临的威胁主要包括哪些？

答：计算机网络上的通信面临的威胁主要包括：

①截获，攻击者从网络上窃听信息。

②中断，攻击者有意中断网络上的通信。

③篡改，攻击者有意更改网络上的信息。

④伪造，攻击者使假的信息在网络上传输。

3. 网络安全的内容主要包括哪些？

答：（1）网络实体安全：如机房的物理条件、物理环境及设施的安全标准，计算机硬件、附属设备及网络传输线路的安装及配置等。（2）软件安全：如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改，不受病毒的侵害等。（3）网络数据安全：如保护网络信息的数据不被非法存取，保护其完整一致等。（4）网络安全管理：如运行时突发事件的安全处理等，包括采取计算机安全技术、建立安全管理制度、开展安全审计、进行风险分析等内容。

4. 什么是黑客？黑客攻击的步骤是什么？

答：黑客是英文 hacker 的音译，原意为热衷于电脑程序的设计者，指对于任何计算机操作系统的奥秘都有强烈兴趣的人。黑客大都是程序员，他们具有操作系统和编程语言方面的高级知识，知道系统中的漏洞及其原因所在，他们不断追求更深的知识，并公开他们的发现，与他人分享，并且没有破坏数据的企图。

黑客攻击的步骤如下：

（1）收集目标计算机的信息。

（2）寻求目标计算机的漏洞和选择合适的入侵方法。

（3）留下“后门”。

（4）清除入侵记录。

5. 什么是防火墙？其功能有哪些？

答：防火墙是一个或一组在两个网络之间执行访问控制策略的系统，包括硬件和软件，目的是保护网络不被可疑人侵扰。本质上，它遵从的是一种允许或阻止业务来往的网络通信安全机制，也就是提供可控的过滤网络通信，只允许授权的通信。

由软件和硬件组成的防火墙应该具有以下功能。

①所有进出网络的通信流都应该通过防火墙。

②所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权。

③理论上说，防火墙是穿不透的。