《计算机网络》课后习题答案

第 1 章 概述

1-1 计算机网络可以向用户提供哪些服务？

答：计算机网络向用户提供的最重要的功能有两个，连通性和共享。

1-2 试简述分组交换的要点。

答：分组交换实质上是在“存储——转发”基础上发展起来的。它兼有电路交换和报文交换的优点。分组交换在线路上采用动态复用技术传送按一定长度分割为许多小段的数据——分组。每个分组标识后，在一条物理线路上采用动态复用的技术，同时传送多个数据分组。把来自用户发端的数据暂存在交换机的存储器内，接着在网内转发。到达接收端，再去掉分组头将各数据字段按顺序重新装配成完整的报文。分组交换比电路交换的电路利用率高，比报文交换的传输时延小，交互性好。

1-3 试从多个方面比较电路交换、报文交换和分组交换的主要优缺点。

答：（1）电路交换 电路交换就是计算机终端之间通信时，一方发起呼叫，独占一条物理线路。当交换机完成接续，对方收到发起端的信号，双方即可进行通信。在整个通信过程中双方一直占用该电路。它的特点是实时性强，时延小，交换设备成本较低。但同时也带来线路利用率低，电路接续时间长，通信效率低，不同类型终端用户之间不能通信等缺点。电路交换比较适用于信息量大、长报文，经常使用的固定用户之间的通信。

（2）报文交换 将用户的报文存储在交换机的存储器中。当所需要的输出电路空闲时，再将该报文发向接收交换机或终端，它以“存储——转发”方式在网内传输数据。报文交换的优点是中继电路利用率高，可以多个用户同时在一条线路上传送，可实现不同速率、不同规程的终端间互通。但它的缺点也是显而易见的。以报文为单位进行存储转发，网络传输时延大，且占用大量的交换机内存和外存，不能满足对实时性要求高的用户。报文交换适用于传输的报文较短、实时性要求较低的网络用户之间的通信，如公用电报网。

（3）分组交换 分组交换实质上是在“存储——转发”基础上发展起来的。它兼有电路交换和报文交换的优点。分组交换在线路上采用动态复用技术传送按一定长度分割为许多小段的数据——分组。每个分组标识后，在一条物理线路上采用动态复用的技术，同时传送多个数据分组。把来自用户发端的数据暂存在交换机的存储器内，接着在网内转发。到达接收端，再去掉分组头将各数据字段按顺序重新装配成完整的报文。分组交换比电路交换的电路利用率高，比报文交换的传输时延小，交互性好。

1-4 为什么说因特网是自印刷术以来人类通信方面最大的变革？

答：因特网缩短了人际交往的时间和空间，改变了人们的生活、工作、学习和交往方式，是世界发生了极大的变化。

1-5 因特网的发展大致分为哪几个阶段？请指出这几个阶段最主要的特点。

答：第一阶段是从单个网络 ARPANRET 向互联网发展的过程。最初的分组交换网 ARPANET 只是一个单个的分组交换网，所有要连接在 ARPANET 上的主机都直接与就近的结点交换机相连。而后发展为所有使用 TCP/IP 协议的计算机都能利用互联网相互通信。

第二阶段是 1985-1993 年，特点是建成了三级结构的因特网

第三阶段是 1993 年至今，特点是逐渐形成了多层次 ISP 结构的因特网。

1-6 简述因特网标准制定的几个阶段。

答：制定英特网的正式标准要经过一下的四个阶段[RFC 2026]：
(1)因特网草案（Internet Draft）。
(2)建议标准（Proposed Standard）。
(3)草案标准（Draft Standard）。
(4)因特网标准（Internet Standard）。

1-7 小写和大些开头的英文名字 internet 和 Internet 在意思上有何重要区别？
答：以小写字母 i 开始的 internet（互联网或互连网）是一个通用名词，它泛指由多个计算机网络互联而成的网络。在这些网络之间的通信协议（即通信规则）可以是任意的。
以大写字母 I 开始的 Internet（因特网）则是一个专有名词，它指当前全球最大的、开放的、由众多网络相互连接而成的特定计算机网络，它采用 TCP/IP 协议族作为通信的规则，其前身是美国的 ARPANET。

1-8 计算机网络都有哪些类别？各种类别的网络都有哪些特点？
答：1、按网络覆盖的地理范围分类：
（1）、局域网：局域网是计算机硬件在比较小的范围内通信线路组成的网络，一般限定在较小的区域内，通常采用有线的方式连接起来。
（2）、城域网：城域网规模局限在一座城市的范围内，覆盖的范围从几十公里至数百公里，城域网基本上是局域网的延伸，通常使用与局域网相似的技术，但是在传输介质和布线结构方面牵涉范围比较广。
（3）、广域网：覆盖的地理范围非常广，又称远程网，在采用的技术、应用范围和协议标准方面有所不同。

2、按传榆介质分类：
（1）、有线网：采用同轴电缆、双绞线，甚至利用又线电视电视电缆来连接的计算机网络，又线网通过"载波"空间进行传输信息，需要用导线来实现。
（2）、无线网：用空气做传输介质，用电磁波作为载体来传播数据。无线网包括：无线电话、语音广播网、无线电视网、微波通信网、卫星通信网。

3、按网络的拓扑结构分类：
（1）、星型网络：各站点通过点到点的链路与中心相连，特点是很容易在网络中增加新的站点，数据的安全性和优先级容易控制，易实现网络监控，但一旦中心节点有故障会引起整个网络瘫痪。
（2）、总线型网络：网络中所有的站点共享一条数据通道，总线型网络安装简单方便，需要铺设的电线最短，成本低，某个站点的故障一般不会影响整个网络，但介质的故障会导致网络瘫痪，总线网安全性低，监控比较困难，增加新站点也不如星型网络容易。
（3）、树型网络：是上述两种网的综合。
（4）、环型网络：环型网容易安装和监控，但容量有限，网络建成后，增加新的站点较困难。
（5）、网状型网络：网状型网络是以上述各种拓扑网络为基础的综合应用。

4、按通信方式分类：
（1）、点对点传输网络：数据以点到点的方式在计算机或通信设备中传输，在一对机器之间通过多条路径连接而成，大的网络大多采用这种方式。

（2）、广播式传输网络：数据在共用通信介质线路中传输，由网络上的所有机器共享一条通信信道，适用于地理范围小的小网或保密要求不高的网络。

5、按网络使用的目的分类：
（1）、共享资源网：使用者可共享网络中的各种资源。
（2）、数据处理网：用于处理数据的网络。
（3）、数据传输网：用来收集、交换、传输数据的网络。

6、按服务方式分类：
（1）、客户机/服务器(C / S)模式：C / S 计算的模式的结构是分散、多层次和具有图形用户接口的 PC 机作为客户机，不同的操作系统或不同的网络操作系统对应不同的语言和开发工具，其工作特点是文件从服务器被下载到工作站上，然后在工作站上进行处理，而基于主机的大型机工作特点是所有处理都发生在主机上。
（2）、浏览器/服务器(B / S)模式：主要特点是它与软硬件平台的无关性，把应用逻辑和业务处理规则放在服务器一侧。
（3）、对等网或称为对等式的网络：对等网可以不要求具备文件服务器，特别是应用在一组面向用户的 PC 机，每台客户机都可以与其他每台客户机实现"平等"对话操作，共享彼此的信息资源和硬件资源，组网的计算机一般类型相同，甚至操作系统也相同，这种网络方式灵活方便，但是较难实现集中管理与控制，安全性也低。

7、按企业和公司管理分类：
（1）、内部网：一般指企业内部网，自成一体形成一个独立的网络。
（2）、内联网：一般指经改造的或新建的企业内部网，采用通用的 TCP / IP 作为通信协议，一般具备自己的 WWW 服务器和安全防护系统，为企业内部服务，不和因特网直接进行连接。
（3）、外联网：采用因特网技术，有自己的 WWW 服务器，但不一定与因特网直接进行连接的网络，同时必须建立防火墙把内联网与因特网隔离开，以确保企业内部信息的安全。
（4）、因特网：因特网是目前最流行的一种国际互联网，在全世界范围内得到应用，结合多媒体的"声、图、文"表现能力，不仅能处理一般数据和文本，而且也能处理语音、声响、静止图象、电视图象、动画和三维图形等。

1-9 计算机网络中的主干网和本地接入网的主要区别是什么？
答：主干网的特点：设施共享；高度综合集成，可应付高密度的业务需求量；工作在可控环境；使用率高；技术演进迅速，以软件为主；成本逐渐下降。
本地接入网特点：设施专用，且分散独立；接入业务种类多，业务量密度低；线路施工难度大，设备运行环境恶劣；使用率低；技术演进迟缓，以硬件为主；网径大小不一，成本与用户有关。

1-10 试在下列条件下比较电路交换和分组交换。要传送的报文共 x（bit），从源站到目的站共经过 k 段链路，每段链路的传播时延为 d（s），数据率为 b（bit/s）。在电路交换时电路的建立时间为 s（s）。在分组交换时分组长度为 p（bit），且各结点的排队等待时间可忽略不计。问在怎样的条件下，分组交换的时延比电路交换的要小？
答：对电路交换，当 t=s 时，链路建立；
当 t=s+x/b，发送完最后一 bit；
当 t=s+x/b+kd，所有的信息到达目的地。

对分组交换，当 t=x/b， 发送完最后一 bit；
为到达目的地，最后一个分组需经过 k-1 个分组交换机的转发，
每次转发的时间为 p/b，
所以总的延迟= x/C+(k-1)p/b+kd
所以当分组交换的时延小于电路交换
x/b+(k-1)p/b+kd＜s+x/b+kd 时，
(k-1)p/C＜s
由上式可知，当 k 和 b 一定时，p 越小，分组交换的时延越小，即需要传送少量数据时（即 p<<x），分组交换的时延较小。

1-11 在上题的分组交换网中，设报文长度和分组长度分别为 x 和（p+h）（bit），其中 p 为分组的数据部分的长度，而 h 为每个分组所带的控制信息固定长度，与 p 的大小无关。通信的两端共经过 k 段链路。链路的数据率为 b（bit/s），但传播时延和结点的排队时间均可忽略不计。若打算使总的时延为最小，问分组的数据部分长度 p 应取为多大？

答：分组个数 x/p，
传输的总比特数：(p+h)x/p
源发送时延：(p+h)x/pb
最后一个分组经过 k-1 个分组交换机的转发，中间发送时延：(k-1)(p+h)/b
总发送时延 D=源发送时延+中间发送时延
D=(p+h)x/pb+(k-1)(p+h)/b
令其对 p 的导数等于 0，求极值
p=√hx/(k-1)

1-12 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？他们的工作方式各有什么特点？

答：边缘部分 由所有连接在因特网上的主机组成。这部分是用户直接使用的，用来进行通信（传送数据、音频或视频）和资源共享。

核心部分 由大量网络和连接 这些网络的路由器组成。这部分是为边缘部分提供服务的(提供连通性和交换）。

在网络边缘的端系统中运行的程序之间的通信方式通常可划分为两大类：客户服务器方式（C/S 方式）即 Client/Server 方式 ，对等方式（P2P 方式）即 Peer-to-Peer 方式

客户(client)和服务器(server)都是指通信中所涉及的两个应用进程。客户服务器方式所描述的是进程之间服务和被服务的关系。客户是服务的请求方，服务器是服务的提供方。被用户调用后运行，在打算通信时主动向远地服务器发起通信（请求服务）。因此，客户程序必须知道服务器程序的地址。不需要特殊的硬件和很复杂的操作系统。 一种专门用来提供某种服务的程序，可同时处理多个远地或本地客户的请求。系统启动后即自动调用并一直不断地运行着，被动地等待并接受来自各地的客户的通信请求。因此，服务器程序不需要知道客户程序的地址。一般需要强大的硬件和高级的操作系统支持。对等连接方式从本质上看仍然是使用客户服务器方式，只是对等连接中的每一个主机既是客户又同时是服务器。

网络核心部分是因特网中最复杂的部分。网络中的核心部分要向网络边缘中的大量主机提供连通性，使边缘部分中的任何一个主机都能够向其他主机通信（即传送或接收各种形式的数据）。在网络核心部分起特殊作用的是路由器(router)。路由器是实现分组交换(packet switching)的关键构件，其任务是转发收到的分组，这是网络核心部分最重要的功能。路由器是实现分组交换(packet switching)的关键构件，其任务是转发收到的分组，这是网络核

心部分最重要的功能

1-13 客户服务方式与对等通信方式的主要区别是什么？有没有相同的地方？

答：客户服务器方式是一点对多点的，对等通信方式是点对点的。被用户调用后运行，在打算通信时主动向远地服务器发起通信（请求服务）。因此，客户程序必须知道服务器程序的地址。系统启动后即自动调用并一直不断地运行着，被动地等待并接受来自各地的客户的通信请求。因此，服务器程序不需要知道客户程序的地址。对等连接方式从本质上看仍然是使用客户服务器方式，只是对等连接中的每一个主机既是客户又同时是服务器。对等连接也需要知道对方的服务器地址。

1-14 计算机网络有哪些常用的性能指标？

答：1.速率

比特（bit）是计算机中数据量的单位，也是信息论中使用的信息量的单位。

Bit 来源于 binary digit，意思是一个“二进制数字”，因此一个比特就是二进制数字中的一个 1 或 0。

速率即数据率(data rate)或比特率(bit rate)是计算机网络中最重要的一个性能指标。速率的单位是 b/s，或 kb/s, Mb/s, Gb/s 等。

速率往往是指额定速率或标称速率。

2.带宽

“带宽”(bandwidth)本来是指信号具有的频带宽度，单位是赫（或千赫、兆赫、吉赫等）。现在“带宽”是数字信道所能传送的“最高数据率”的同义语，单位是“比特每秒”，或 b/s (bit/s)。

3.吞吐量

吞吐量(throughput)表示在单位时间内通过某个网络（或信道、接口）的数据量。

吞吐量更经常地用于对现实世界中的网络的一种测量，以便知道实际上到底有多少数据量能够通过网络。

吞吐量受网络的带宽或网络的额定速率的限制。

4.时延

传输时延（发送时延 ）　　发送数据时，数据块从结点进入到传输媒体所需要的时间。也就是从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕所需的时间。

5.时延带宽积

6.往返时间 RTT

7.利用率

1-15 假定网络的利用率到达了 90%。试估算已选现在的网络时延是他的最小值的多少倍？

答：D0 表示网络空闲时的时延，D 表示当前网络的时延。U 为利用率

则： D=D0/(1-U) 即 D=10 D0 。

1-16 计算机通信网有哪些非性能特征？计算机通信网性能指标与非性能特征有什么区别？

答：计算机通信网非性能特征有：费用、质量、标准化、可靠性、可扩展性和可升级性、易于管理和维护。

计算机通信网性能指标有：速率、带宽、吞吐量、时延、时延带宽积、往返时间、利用率。

性能指标指的是与通信网络本身性能相关的指数，而非性能特征与其本身无直接关系。

1-17 收发两端之间的传输距离为 1000km，信号在媒体上的传播速率为 2.3×108 。试计算以下两种情况的发送时延和传播时延：

（1） 数据长度为 107bit，数据发送速率为 100kbit/s，传播距离为 1000km，信号在媒体上的传播速率为 2×108m/s。

（2） 数据长度为 103bit，数据发送速率为 1Gbit/s，传输距离和信号在媒体上的传播速率同上。

答：（1）：发送延迟=107/（100×1000）=100s

传播延迟=1000×1000/（2×108）=5×10-3s=5ms

（2）：发送延迟=103/（109）=10-6s=1us

传播延迟=1000×1000/（2×108）=5×10-3s=5ms

1-18 、假设信号在媒体上的传播速率为 2.3×108m/s。媒体长度 l 分别为：

(1) 10cm(网卡)

(2) 100m(局域网)

(3) 100km(城域网)

(4) 5000km(广域网)

试计算当数据率为 Mb/s1 和 10Gb/s 时在以上媒体中正在传播的比特数。

答：传播时延=信道长度/电磁波在信道上的传播速率

时延带宽积=传播时延*带宽

（1）0.1m/2.3/108×1×108b/s=0.000435bit

（2）100m/2.3/108×1×108b/s=0.435bit

（3）100000/2.3/108×1×108=435bit

（4）5×106/2.3/108×1×108=21739bit

1-19、长度为 100 字节的应用层数据交给运输层传送，需加上 20 字节的 TCP 首部。再交给网络层传送，需加上 20 字节的 IP 首部。最后交给数据链路层的以太网传送，加上首部和尾部 18 字节。试求数据的传输效率。

若应用层数据长度为 1000 字节，数据的传输效率是多少？

答：数据长度为 100 字节时

传输效率=100/（100+20+20+18）=63.3%

数据长度为 1000 字节时，

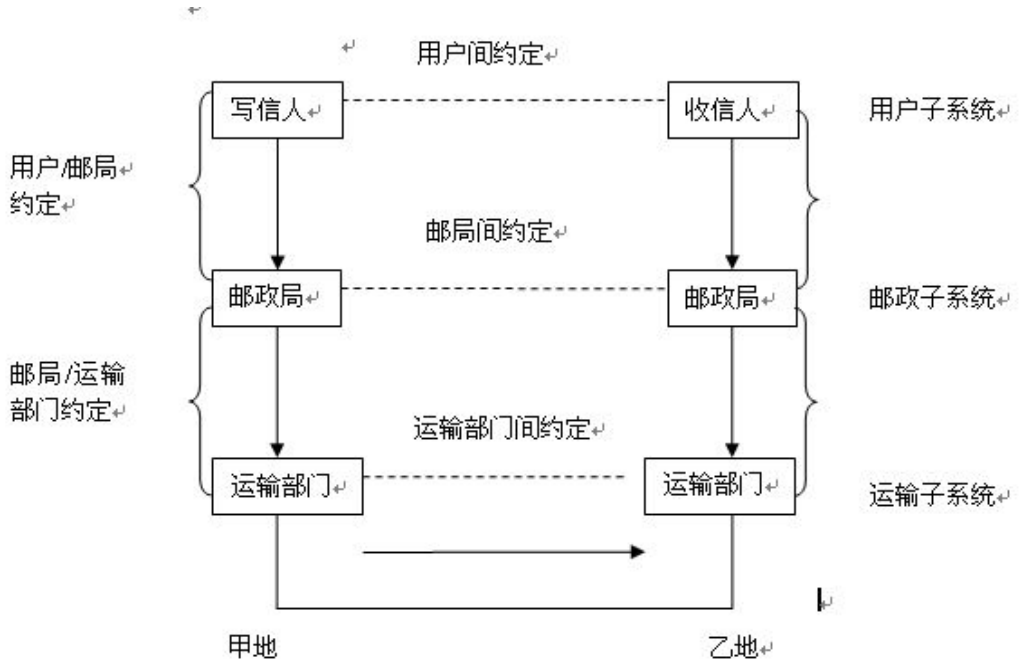
传输效率=1000/（1000+20+20+18）=94.5%

1-20 网络体系结构为什么要采用分层次的结构？试举出一些与分层体系结构的思想相似的日常生活。

答：网络体系结构采用分层的结构，可以减少协议设计的复杂性，使得各层之间是独立的，增强灵活性，使得网络体系结构上可以分割开，易于实现和维护，同时促进标准化工作。

日常生活中，比如，甲、乙两地两人 a、b 通信，a 将写好的信交给甲地邮局，甲地邮局经过交通部门将信邮至乙地邮局，b 再从乙地邮局取信。这相当于一个三层结构，如下图所示

虽然两个用户、两个邮政局、两个运输部门分处甲、乙两地，但是它们都分别对应同等机构，同属一个子系统，而同处一地的不同机构则不再一个子系统内，而且它们之间的关系是服务与被服务的关系。



1-21 协议与服务有何区别？有何关系？

答：协议是水平的，服务是垂直的。

协议是“水平的”， 即协议是控制对等实体之间的通信的规则。服务是“垂直的”， 即服务是由下层向上层通过层间接口提供的。

协议与服务的关系

在协议的控制下，上层对下层进行调用，下层对上层进行服务，上下层间用交换原语交换信息。同层两个实体间有时有连接。

1-22 网络协议的三个要素是什么？各有什么含义？

答：在计算机网络中要做到有条不紊地交换数据，就必须遵守一些事先约定好的规则。

这些为进行网络中的数据交换而建立的规则、标准或约定即称为网络协议。一个网络协议要由以下三个要素组成：

（1）语法，即数据与控制信息的结构或格式；

（2）语义，即需要发出何种控制信息，完成何种动作以及做出何种应答；

（3）同步，即事件实现顺序的详细说明。

对于非常复杂的计算机网络协议，其结构最好采用层次式的。

1-23 为什么一个网络协议必须把各种不利的情况都考虑到？

答：因为网络协议如果不全面考虑不利情况，当情况发生变化时，协议就会保持理想状况，一直等下去！就如同两个朋友在电话中约会好，下午 3 点在公园见面，并且约定不见不撒。这个协议就是很不科学的，因为任何一方如果有耽搁了而来不了，就无法通知对方，而另一方就必须一直等下去！所以看一个计算机网络是否正确，不能只看在正常情况下是否正确，而且还必须非常仔细的检查协议能否应付各种异常情况。

1-24 试述五层协议的网络体系结构的要点，包括各层的主要功能。

答：所谓五层协议的网络体系结构是为便于学习计算机网络原理而采用的综合了 OSI 七层模型和 TCP/IP 的四层模型而得到的五层模型。五层协议的体系结构见图 1-1 所示。

图 1-1 五层协议的体系结构

各层的主要功能：

（1）应用层

应用层确定进程之间通信的性质以满足用户的需要。应用层不仅要提供应用进程所需要的信息交换和远地操作，而且还要作为互相作用的应用进程的用户代理（user agent),来完成一些为进行语义上有意义的信息交换所必须的功能。

(2）运输层

任务是负责主机中两个进程间的通信。

因特网的运输层可使用两种不同的协议。即面向连接的传输控制协议 TCP 和无连接的用户数据报协议 UDP。

面向连接的服务能够提供可靠的交付。

无连接服务则不能提供可靠的交付。只是 best-effort delivery.

(3)网络层

网络层负责为分组选择合适的路由，使源主机运输层所传下来的分组能够交付到目的主机。

（4）数据链路层

数据链路层的任务是将在网络层交下来的数据报组装成帧（frame)，在两个相邻结点间的链路上实现帧的无差错传输。

（5）物理层

物理层的任务就是透明地传输比特流。

“透明地传送比特流”指实际电路传送后比特流没有发生变化。

物理层要考虑用多大的电压代表“1”或“0”，以及当发送端发出比特“1”时，接收端如何识别出这是“1”而不是“0”。物理层还要确定连接电缆的插头应当有多少根脚以及各个脚如何连接。

1-25 试举出日常生活中有关“透明”这种名词的例子。

答:“透明”是指某一个实际存在的事物看起来却好像不存在一样。书上举例如:你看不见在你面前有 100%透明的玻璃的存在。

1-26 试解释下列名词：协议栈、实体、对等层、协议数据单元、服务访问点、客户、服务器、客户-服务器方式。

答：协议栈：指计算机网络体系结构采用分层模型后，每层的主要功能由对等层协议的运行来实现，因而每层可用一些主要协议来表征，几个层次画在一起很像一个栈的结构。

实体：表示任何可发送或接收信息的硬件或软件进程。在许多情况下，实体是一个特定的软件模块。

对等层：在网络体系结构中，通信双方实现同样功能的层。

协议数据单元：对等层实体进行信息交换的数据单位。

服务访问点：在同一系统中相邻两层的实体进行交互（即交换信息）的地方。服务访问点SAP是一个抽象的概念，它实体上就是一个逻辑接口。
客户、服务器：客户和服务器都是指通信中所涉及的两个应用进程。客户-服务器方式所描述的是进程之间服务和被服务的关系。客户是服务请求方，服务器是服务提供方。
客户-服务器方式：客户-服务器方式所描述的是进程之间服务和被服务的关系，当客户进程需要服务器进程提供服务时就主动呼叫服务进程，服务器进程被动地等待来自客户进程的请求。

1-27 试解释everything over IP和IP over everything的含义。
答：everything over IP：即IP为王，未来网络将由IP一统天下。未来的通信网既已肯定以数据信息业务为重心，并普遍使用互联网规约IP，那么网上信息业务宜一律使用IP，即所谓everything over IP。
IP over everything：在现在的电通信网过渡到光通信网的过程中，IP、ATM、WDM会配合使用，渐渐过渡，既是IP over everything。

第 2 章 物理层

2-01 物理层要解决什么问题？物理层的主要特点是什么？

（1）物理层要解决的主要问题：

①.物理层要尽可能屏蔽掉物理设备、传输媒体和通信手段的不同，使上面的数据链路层感觉不到这些差异的存在，而专注于完成本曾的协议与服务。

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。

（2）物理层的主要特点：

①.由于在 OSI 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锁采用。加之，物理层协议涉及的范围广泛，所以至今没有按 OSI 的抽象模型制定一套心的物理层协议，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。

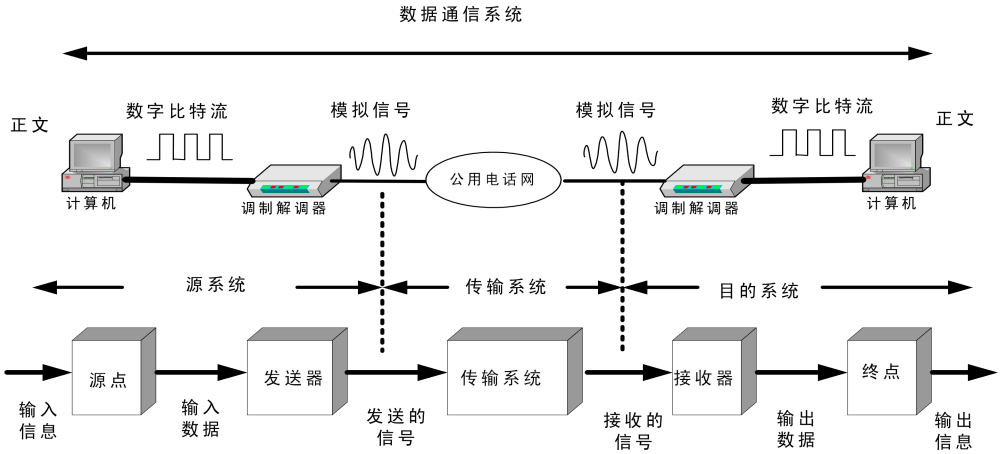
2-02 规程与协议有什么区别？

答：在数据通信的早期，对通信所使用的各种规则都称为“规程”（procedure），后来具有体系结构的计算机网络开始使用“协议”（protocol）这一名词，以前的“规程”其实就是“协议”，但由于习惯，对以前制定好的规程有时仍常用旧的名称“规程”。

2-03 试给出数据通信系统的模型并说明其主要组成构件的作用。

答：一个数据通信系统可划分为三大部分：

源系统（或发送端）、传输系统（或传输网络）、和目的系统（或接收端）。



数据通信系统的模型

源系统一般包括以下两个部分：

•源点：源点设备产生要传输的数据。例如正文输入到 PC 机，产生输出的数字比特流。

•发送器：通常源点生成的数据要通过发送器编码后才能在传输系统中进行传输。例如，调制解调器将 PC 机输出的数字比特流转换成能够在用户的电话线上传输的模拟信号。

•接收器：接收传输系统传送过来的信号，并将其转换为能够被目的设备处理的信息。例如，调制解调器接收来自传输线路上的模拟信号，并将其转换成数字比特流。
•终点：终点设备从接收器获取传送过来的信息。

2-04 试解释以下名词：数据、信号、模拟数据、模拟信号、基带信号、带通信号、数字数据、数字信号、码元、单工通信、半双工通信、全双工通信、串行传输、并行传输。

答：数据：是运送信息的实体。
信号：则是数据的电气的或电磁的表现。
模拟数据：运送信息的模拟信号。
模拟信号：连续变化的信号。
基带信号：来自信源的信号。
带通信号：经过载波调制后的信号。
数字信号：取值为有限的几个离散值的信号。
数字数据：取值为不连续数值的数据。
码元：在使用时间域的波形表示数字信号时，代表不同离散数值的基本波形
单工通信：即只有一个方向的通信而没有反方向的交互。
半双工通信：即通信和双方都可以发送信息，但不能双方同时发送（当然也不能同时接收）。这种通信方式是一方发送另一方接收，过一段时间再反过来。
全双工通信：即通信的双方可以同时发送和接收信息。
基带信号（即基本频带信号）——来自信源的信号。像计算机输出的代表各种文字或图像文件的数据信号都属于基带信号。
带通信号——把基带信号经过载波调制后，把信号的频率范围搬移到较高的频段以便在信道中传输（即仅在一段频率范围内能够通过信道）。

2-05 物理层的接口有哪几个特性？各包含什么内容？

答：（1）机械特性：指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。

2-06 数据在信道中的传输速率受哪些因素的限制？信噪比能否任意提高？香农公式在数据通信中的意义是什么？“比特/秒”和“码元/秒”有何区别？

答：限制码元在信道上的传输速率的因素有以下两个：

（1）在任何信道中，码元传输速率是有上限的，传输速率超过此上限，就会出现严重的码元间串扰的问题，使接收端对码元的判决（即识别）成为不可能。

（2）由于噪声会使接收端对码元的判决产生错误（1 判决为 0 或 0 判决为 1）。所以信噪比要限制在一定范围内。由香农公式可知，信息传输速率由上限。

信噪比越大，量化性能越好；均匀量化的输出信噪比随量化电平数的增加而提高；非均匀量化的信号量噪比，例如 PCM 随编码位数 N 指数规律增长，DPCM 与频率有关等。但实际信噪比不能任意提高，都有一定限制。例如增加电平数会导致接收机的成本提高，制作工艺复杂等。

香农公式的意义在于：只要信息传输速率低于信道的极限信息传输速率，就一定可以找到某种方法来实现无差错的传输。

比特/秒是指信息传输速率，每秒钟传送的信息量；码元/秒是码元传输速率，每秒钟传送的码元个数。两者在二进制时相等。在多进制时，信息传输速率要乘以 log 以 2 为底的进制数等于码元传输速率

2-07 假定某信道受奈氏准则限制的最高码元速率为 2000 码元/秒。如果采用振幅调制，把码元的振幅划分为 16 个不同等级来传送，那么可以获得多高的数据率（b/s）？

答：80000 b/s

2-08 假定要用 3kHz 贷款的电话信道传送 64kb/s 的数据（无差错传输），试问这个信道应该具有多高的信噪比（分别用比值和分贝来表示），这个结果说明什么问题？

答：S/N=64.2dB　　是个信噪比很高的信道

2-09 用香农公式计算一下：假定信道带宽为 3100Hz，最大信息传输速率为 35kb/s，那么若想使最大信息传输速率增加 60%。问信噪比 S/N 应增大到多少倍？如果在刚才计算出的基础上将信噪比 S/N 再增大到 10 倍，问最大信息传输速率能否再增加 20%？

答：奈氏准则：每赫带宽的理想低通信道是最高码元传输速率是每秒 2 个码元。香农公式则表明了信道的带宽或信道中的信噪比越大，则信息的极限传输速率就越高。根据香农公式，计算信道的极限信息传输速率 C 为：$C=\log_2(1+S/N)$ b/s;根据公式，可以计算出，信噪比 S/N 应增大到 100 倍。如果在此基础上将信噪比 S/N 再增大 10 倍，最大信息速率只能再增加 18.5%左右。

2-10 常用的传输媒体有哪几种？各有何特点？

答：常见的传输媒体有以下几种

1.双绞线

双绞线分屏蔽双绞线和无屏蔽双绞线。由两根相互绝缘的导线组成。可以传输模拟信号，也可以传输数字信号，有效带宽达 250kHz，通常距离一般为几道十几公里。导线越粗其通信距离越远。在数字传输时，若传输速率为每秒几兆比特，则传输距离可达几公里。一般用作电话线传输声音信号。虽然双绞线容易受到外部高频电磁波的干扰，误码率高，但因为其价格便宜，且安装方便，既适于点到点连接，又可用于多点连接，故仍被广泛应用。

2.同轴电缆

同轴电缆分基带同轴电缆和宽带同轴电缆，其结构是在一个包有绝缘的实心导线外，再套上一层外面也有一层绝缘的空心圆形导线。由于其高带宽（高达 300~400Hz）、低误码率、性能价格比高，所以用作 LAN 中。同轴电缆的最大传输距离随电缆型号和传输信号的不同而不同，由于易受低频干扰，在使用时多将信号调制在高频载波上。

3.光导纤维

光导纤维以光纤维载体，利用光的全反向原理传播光信号。其优点是直径小、质量轻：传播频带款、通信容量大：抗雷电和电磁干扰性能好，五串音干扰、保密性好、误码率低。但光电接口的价格较昂贵。光纤被广泛用于电信系统铺设主干线。

4.无线电微波通信

无线电微波通信分为地面微波接力通信和卫星通信。其主要优点是频率高、频带范围宽、通信信道的容量大；信号所受工业干扰较小、传播质量高、通信比较稳定；不受地理环境的影响，建设投资少、见效快。缺点是地面微波接力通信在空间是直线传播，传输距离受到限制，一般只有 50km，隐蔽性和保密性较差；卫星通信虽然通信距离远且通信费用与通信距离无关，但传播时延较大，技术较复杂，价格较贵。

2-11 假定有一种双绞线衰减是 0.7db/km,若容许有 20db 的衰减,试问使用这种双绞线的链路的工作距离有多长？如果要使这种双绞线的工作距离增大到 100 公里，问应该使衰减降低到多少？

答：在此频率下可的传输距离=20/0.7≈28.57（km）。

工作距离增大到 100 公里，衰减应该为 20/100=0.2db/m

2-12 试计算工作在 1200nm 到 1400nm 以及 1400 到 1600 之间（波长）的光波的频带宽度。假定光在光纤中的传播速率为 $2x10^8$。

答：$2x10^8/1200 \times 10^{-9}-2x10^8/1400 \times 10^{-9}=2.381 \times 10^{13}= 23.8THZ$

$2x10^8/1400 \times 10^{-9}-2x10^8/1600 \times 10^{-9}=1.786 \times 10^{13}= 17.86THZ$

2-13 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：信道复用的目的是让不同的计算机连接到相同的信道上,以共享信道资源。在一条传输介质上传输多个信号,提高线路的利用率，降低网络的成本。这种共享技术就是多路复用技术。

频分复用（FDM，Frequency Division Multiplexing）就是将用于传输信道的总带宽划分成若干个子频带（或称子信道），每一个子信道传输 1 路信号。频分复用要求总频率宽度大于各个子信道频率之和，同时为了保证各子信道中所传输的信号互不干扰，应在各子信道之间设立隔离带，这样就保证了各路信号互不干扰（条件之一）。频分复用技术的特点是所有子信道传输的信号以并行的方式工作，每一路信号传输时可不考虑传输时延，因而频分复用技术取得了非常广泛的应用。

时分复用（TDM，Time Division Multiplexing）就是将提供给整个信道传输信息的时间划分成若干时间片（简称时隙），并将这些时隙分配给每一个信号源使用，每一路信号在自己的时隙内独占信道进行数据传输。时分复用技术的特点是时隙事先规划分配好且固定不变，所以有时也叫同步时分复用。其优点是时隙分配固定，便于调节控制，适于数字信息的传输；缺点是当某信号源没有数据传输时，它所对应的信道会出现空闲,而其他繁忙的信道无法占用这个空闲的信道,因此会降低线路的利用率。时分复用技术与频分复用技术一样，有着非常广泛的应用，电话就是其中最经典的例子，此外时分复用技术在广电也同样取得了广泛地应用，如 SDH，ATM，IP 和 HFC 网络中 CM 与 CMTS 的通信都是利用了时分复用的技术。

2-14 试写出下列英文缩写的全文，并进行简单的解释。

FDM，TDM，STDM，WDM，DWDM，CDMA，SONET，SDH，STM-1，OC-48

答：

FDM(frequency division multiplexing)频分复用，同一时间同时发送多路信号。所有的用户可以在同样的时间占用不同的带宽资源。

TDM(Time Division Multiplexing)时分复用，将一条物理信道按时间分成若干时间片轮流地给多个用户使用，每一个时间片由复用的一个用户占用，所有用户在不同时间占用同样的频率宽度。

STDM(Statistic Time Division Multiplexing)统计时分复用，一种改进的时分复用。不像时分复用那样采取固定方式分配时隙，而是按需动态地分配时时隙。

WDM(Wave Division Multiplexing)波分复用，在光信道上采用的一种频分多路敷衍的变种，即光的频分复用。不同光纤上的光波信号（常常是两种光波信号）复用到一根长距离传输的光纤上的复用方式。
DWDM(Dense Wave Division Multiplexing)密集波分复用，使用可见光频谱的宽带特征在单个光纤上同时传输多种光波信号的技术。DWDM 可以利用一根光纤同时传输多个波长，多路高速信号可以在光纤介质中同时传输，每路信号占用不同波长。
CDMA(Code Wave Division Multiplexing)码分多址，是采用扩频的码分多址技术。用户可以在同一时间、同一频段上根据不同的编码获得业务信道。
SONET(Synchronous Optical Network)同步光纤网，是以分级速率从 155Mb/s 到 2.5Gb/s 的光纤数字化传输的美国标准，它支持多媒体多路复用，允许声音、视频和数据格式与不同的传输协议一起在一条光纤线路上传输。
SDH(Synchronous Digital Hierarchy)同步数字系列指国际标准同步数字系列。SDH 简化了复用和分用技术，需要时可直接接入到低速支路，而不经过高速到低速的逐级分用，上下电路方便。
STM-1(Synchronous Transfer Module)第 1 级同步传递模块，SDH 的基本速率，相当于 SONET 体系中的 OC-3 速率。
OC-48(Optical Carrier)第 48 级光载波，是 SONET 体系中的速率表示，对应于 SDH 的 STM-16 速率，常用近似值 2.5Gb/s.

2-15 码分 CDMA 为什么可以使所有用户在同样的时间使用同样的频带进行通信而不会相互干扰？这种复用方法有何优缺点？

答:因为用户在使用 CDMA 通信时，各用户使用经过特殊挑选的不同码型传送信息时，用一个带宽远大于信号带宽的高速伪随机码进行调制，使原数据信号的带宽被扩展，再经载波调制并发送出去。接收端由使用完全相同的伪随机码，与接收的带宽信号作相关处理，把带宽信号换成原信息书籍的窄带信号即解扩、以实现信息通信。各用户之间不会造成干扰。

这种复用方法的优点 ：频谱利用率高，容量大；覆盖范围大；有很强的抗干扰能力，其频谱类似于白噪声，传送的信号不易被敌人发现；采用 CDMA 可提高通信的话音质量和数据传输的可靠性，减少对通信的影响；网络成本低；降低手机的平均发射功率等等。
缺点是：需要为各站分配不同互相正交的码片序列；地域受线路影响，不是每个地方都能用，安装时间长等。

2-16 共有 4 个站进行码分多址 CDMA 通信。4 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：（-1 +1 -3 +1 -1 -3 +1 +1）。问哪个站发送数据了？发送数据的站发送的 1 还是 0？

答：S·A=（＋1－1＋3＋1－1＋3＋1＋1）／8=1， A 发送 1
S·B=（＋1－1－3－1－1－3＋1－1）／8=－1， B 发送 0
S·C=（＋1＋1＋3＋1－1－3－1－1）／8=0， C 无发送
S·D=（＋1＋1＋3－1＋1＋3＋1－1）／8=1， D 发送 1

2-17 试比较 xDSL，HFC 以及 FTTx 接入技术的优缺点。

答：xDSL 技术就是用数字技术对现有的模拟电话用户线进行改造，使它能够承载宽带业务。成本低，易实现，但带宽和质量差异性大。

HFC 网的最大的优点具有很宽的频带，并且能够利用已经有相当大的覆盖面的有线电视网。要将现有的 450 MHz 单向传输的有线电视网络改造为 750 MHz 双向传输的 HFC 网需要相当的资金和时间。

FTTx（光纤到……）这里字母 x 可代表不同意思。可提供最好的带宽和质量、但现阶段线路和工程成本太大。

2-18 为什么 ADSL 技术中，在不到 1MHz 的带宽中却可以传递速率高达每秒几个兆比？

答：靠先进的编码，使得每秒传送一个码元就相当于每秒传送多个比特。

2-19 什么是 EPON 和 GPON?

答：EPON 是 以太网无源光网络。

GPON 是 Gbit 容量无源光网络。

第 3 章 数据链路层

3-01 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”的区别何在？

答： （1）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。

（2）“电路接通了”表示链路两端的结点交换机已经开机，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、确认和重传等功能，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，物理电路连接不一定跟着断开连接。

3-02、数据链路层中的链路控制包括哪些功能？试讨论数据链路层做成可靠的链路层有哪些优点和缺点。

答： 数据链路层中的链路控制包括以下功能：链路管理；帧同步；流量控制；差错控制；将数据和控制信息分开；透明传输；寻址。

数据链路层做成可靠的链路层的优点和缺点：所谓“可靠传输”就是：数据链路层的发送端发送什么，在接收端就收到什么。这就是收到的帧并没有出现比特差错，但却出现了帧丢失、帧重复或帧失序。以上三种情况都属于“出现传输差错”，但都不是这些帧里有“比特差错”。“无比特差错”

与“无传输差错”并不是同样的概念。在数据链路层使用 CRC 检验，能够实现无比特差错的传输，但这不是可靠的传输。

3-03、网络适配器的作用是什么？网络适配器工作在哪一层？

答： 络适配器能够对数据的串行和并行传输进行转换,并且能够对缓存数据进行出来,实现以太网协议,同时能够实现帧的传送和接受,对帧进行封闭等.网络适配器工作在物理层和数据链路层。

3-04、数据链路层的三个基本问题（帧定界、透明传输和差错检测）为什么都必须加以解决？

答： 帧定界使收方能从收到的比特流中准确地区分出一个帧的开始和结束在什么地方；

透明传输使得不管所传数据是什么样的比特组合，都应当能够在链路上传送，因此很重要；

差错控制主要包括差错检测和差错纠正,旨在降低传输的比特差错率,因此也必须解决。

3-05、如果在数据链路层不进行帧定界，会发生什么问题？

答： 如果在数据链路层不进行帧定界，将发生帧数据错误，造成数据混乱，通信失败。

3-06、PPP 协议的主要特点是什么？为什么 PPP 不使用帧的编号？PPP 适用于什么情况？为什么 PPP 协议不能使数据链路层实现可靠传输？

答： 主要特点：

1、点对点协议，既支持异步链路，也支持同步链路。

2、PPP 是面向字节的。
PPP 不采用序号和确认机制是出于以下的考虑：
1、若使用能够实现可靠传输的数据链路层协议（如 HDLC），开销就要增大。在数据链路层出现差错的概率不大时，使用比较简单的 PPP 协议较为合理。
2、在因特网环境下，PPP 的信息字段放入的数据是 IP 数据报。假定我们采用了能实现可靠传输但十分复杂的数据链路层协议，然而当数据帧在路由器中从数据链路层上升到网络层后，仍有可能因网络授拥塞而被丢弃。因此，数据链路层的可靠传输并不能保证网络层的传输也是可靠的。
3、PPP 协议在帧格式中有帧检验序列 FCS 安段。对每一个收到的帧，PPP 都要使用硬件进行 CRC 检验。若发现有差错，则丢弃该帧（一定不能把有差错的帧交付给上一层）。端到端的差错检测最后由高层协议负责。因此，PPP 协议可保证无差错接受。
PPP 协议适用于用户使用拨号电话线接入因特网的情况。
PPP 协议不能使数据链路层实现可靠传输的原因：PPP 有 FCS 来确保数据帧的正确性，如果错误则上报错误信息来确保传输的可靠性。当然它和其他 L2 协议一样，没有 TCP 的 ACK 机制，这也是传输层以下协议所具有的特性，以便于提高网络的性能。

3-07 要发送的数据为 1101011011。采用 CRC 的生成多项式是 P(x)=x4+x+1 。试求应添加在数据后面的余数。
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？
答：添加的检验序列为 1110 （11010110110000 除以 10011） 数据在传输过程中最后一个 1 变成了 0，11010110101110 除以 10011，余数为 011，不为 0，接收端可以发现差错。
数据在传输过程中最后两个 1 都变成了 0，11010110001110 除以 10011，余数为 101，不为 0，接收端可以发现差错。

3-08．要发送的数据为 101110。采用 CRC 的生成多项式是 P(X)=X3+1。试求应添加在数据后面的余数。
解：余数是 011。

3-09． 一个 PPP 帧的数据部分（用十六进制写出）是 7D 5E FE 27 7D 5D 7D 5D 65 7D 5E。试问真正的数据是什么（用十六进制写出）？
答：7E FE 27 7D 7D 65 7E。

3-10．PPP 协议使用同步传输技术传送比特串 0110111111111100。试问经过零比特填充后变成怎样的比特串？若接收端收到的 PPP 帧的数据部分是 000111011111O111111O110，问删除发送端加入的零比特后变成怎样的比特串？
答：第一个比特串：经过零比特填充后编程 011011111011111000（加上下划线的 0 是填充的）。另一个比特串：删除发送端加入的零比特后变成 000111011111-11111-110（连字符表示删除了 0）。

3-11．试分别讨论以下各种情况在什么条件下是透明传输，在什么条件下不是透明传输。（提示：请弄清什么是“透明传输”，然后考虑能否满足其条件。）
（1）普通的电话通信。
（2）电信局提供的公用电报通信。

（3）因特网提供的电子邮件服务。

答：(1)由于电话系统的带宽有限，而且还有失真，因此电话机两端的输入声波和输出声波是有差异的。在“传送声波”这个意义上讲，普通的电话通信不是透明传输。但对“听懂说话的意思”来讲，则基本上是透明传输。但也有时个别语音会听错，如单个的数字 1 和 7.这就不是透明传输。

（2）一般说来，由于电报通信的传输是可靠的，接收的报文和发送的报文是一致的，因此应当是透明传输。但如果有人到电信局发送“1849807235”这样的报文，则电信局会根据有关规定拒绝提供电报服务（电报通信不得为公众提供密码通信服务）。因此，对于发送让一般人看不懂意思的报文，现在的公用电报通信则不是透明通信。

（3）一般说来，电子邮件时透明传输。但有时不是。因为国外有些邮件服务器为了防止垃圾邮件，对来自某些域名(如.cn)的邮件一律阻拦掉。这就不是透明传输。有些邮件的附件在接收人的电脑上打不开。这也不是透明传输。

3-12.PPP 协议的工作状态有哪几种？当用户要使用 PPP 协议和 ISP 建立连接进行通信需要建立哪几种连接？每一种连接解决什么问题？

答：PPP 协议的工作状态分为：“链路终止”状态，“链路静止”状态，“链路建立”状态，“鉴别”状态，“网络层协议”状态，“链路打开”状态。

用户要使用 PPP 协议和 ISP 建立连接进行通信需要建立的连接为： 链路静止，链路建立，鉴别，网络层协议，链路打开。链路静止时，在用户 PC 机和 ISP 的路由器之间并不存在物理层的连接。链路建立时，目的是建立链路层的 LCP 连接。

鉴别时，只允许传送 LCP 协议的分组、鉴别协议的分组以及监测链路质量的分组。网络层协议时，PPP 链路的两端的网络控制协议 NCP 根据网络层的不同协议无相交换网络层特定的网络控制分组。链路打开时，链路的两个 PPP 端点可以彼此向对方发送分组。

3-13 局域网的主要特点是什么？为什么局域网采用的广播通信通信方式而广域网不采用呢？

答：（1）局域网的主要特点。

从功能的角度来看，局域网具有以下几个特点：

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；

1. 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联网,如一座楼或几种的建筑群内。一般来说,局域网的覆盖范围约为 10m~10km 内或更大一些；
2. 传输速率高。局域网的传输速率一般为 1~100Mb/s，能支持计算机之间的告诉通信，所以时延较低。
3. 误码率低，因近距离传输，所以误码率很低，一般在 10^{-8}～10^{-11}之间。
4. 多采用分布式控制和广播式通信。在局域网中各站是平等关系而不是主从关系，可以进行广播或组播。

从网络的体系结构和传输控制规程来看，局域网也有自己的特点：

1. 底层协议简单。在局域网中，由于距离短、时延小、成本低、传输速率高、可靠性高，因此信道利用率已不是人们考虑的主要因素，所以底层协议较简单。
2. 不单独设立网络层。局域网的拓扑结构多采用总线型、环型和星型等共享信道，网内一般不需要中间转接，流量控制和路由选择功能大为简化，通常在局域网不单独设立网络层。因此，局域网的体系结构仅相当于 OSI/RM 的最低两层。
3. 采用多种媒体访问控制技术。由于采用共享广播信道，而信道又可用不同的传输媒体，

所以局域网面对的是多源、多目的链路管理的问题。由此引发出多种媒体访问控制技术。

（2）局域网采用广播通信是因为局域网中的机器都连接到同一条物理线路，所有主机的数据传输都经过这条链路，采用的通信方式是将主机要发送的数据送到公用链路上，发送至所有的主机，接收端通过地址对比，接收法网自己的数据，并丢弃其他数据的方式。广域网是由更大的的地理空间、更多的主机构成的，若要将广播用于广域网，可能会导致网络无法运行。首先，主机间发送数据时，将会独自占用通信链路，降低了网络的使用率；另一方面，主机 A 向主机 B 发送数据时，是想网络中所有的主机发送数据，当主机数目非常多时，将严重消耗主机的处理能力。同时也造成了数据的无效流动；再次，极易产生广播风暴，是网络无法运行。

3-14　常用的局域网的网络拓扑有哪些种类？现在最流行的是哪种结构？为什么早期的以太网选择总线拓扑结构而不使用星形拓扑结构，但现在却改为使用星形拓扑结构？

答：常用的局域网的网络拓扑有（1）总线网 （2）星形网 （3）环形网 （4）树形网。

现在最流行的是星形网。

当时很可靠的星形拓扑结构较贵。人们都认为无源的总线结构更加可靠，但是实践证明，连接有大量站点的总线式以太网很容易出现故障，而现在专用的 ASIC 芯片的使用可以将星形结构的集线器做得非常可靠。因此现在的以太网一般都是用星形结构的拓扑结构。

3-15　什么叫做传统以太网？以太网有哪两个主要标准？

答：以太网是当今现有局域网采用的最通用的通信协议标准，组建于七十年代早期。Ethernet(以太网）是一种传输速率为 10Mbps 的常用局域网（LAN）标准。在以太网中，所有计算机被连接一条同轴电缆上，采用具有冲突检测的载波感应多处访问（CSMA/CD）方法，采用竞争机制和总线拓朴结构。基本上，以太网由共享传输媒体，如双绞线电缆或同轴电缆和多端口集线器、网桥或交换机构成。在星型或总线型配置结构中，集线器/交换机/网桥通过电缆使得计算机、打印机和工作站彼此之间相互连接。

有 DIX Ethernet V2 标准和 802.3 标准。

3-16　数据率为 10Mb/s 的以太网在物理媒体上的码元传输速率是多少码元/秒？

答：码元传输速率即为波特率。以太网使用曼彻斯特编码，这就意味着发送的每一位都有两个信号周期。标准以太网的数据速率是 10Mb/s，因此波特率是数据率的两倍，即 20M 波特。

3-17　为什么 LLC 子层的标准已制定出来了但现在却很少使用？

答：为了是数据链路层能更好的使用多种局域网标准，802 委员会就将局域网的数据链路层拆成两个子层，即逻辑链路控制 LLC 子层和媒体介入控制 MAC 子层。与接入到传输媒体有关的内容都放在 MAC 子层，而 LLC 子层则与传输媒体无关，不管采用何种协议的局域网对 LLC 子层来说都是透明的。

由于现在 TCP/IP 体系经常是用的局域网是 DIX Ethernet V2 而不是 802.3 标准中的几种局域网。因此现在 802 委员会制定的逻辑链路控制子层的作用已经不大了，很多厂商生产的网卡上都仅装有 MAC 协议而没有 LLC 协议。所以 LLC 子层的标准现在已经很少使用了。

3-18　试说明 10BASE-T 中的“10”、“BASE”和“T”所代表的意思。

答：10BASE-T：“10”表示数据率为 10Mb/s，“BASE”表示电缆上的信号是基带信号，“T”表示使用双绞线的最大长度是 500m。

3-19　以太网使用的 CSMA/CD 协议是以争用方式接入到共享信道。这与传统的时分复用 TDM 相比优缺点如何？

答：CSMA/CD 是一种动态的媒体随机接入共享信道方式，而传统的时分复用 TDM 是一种静态的划分信道，所以对信道的利用，CSMA/CD 是用户共享信道，更灵活，可提高信道的利用率，不像 TDM，为用户按时隙固定分配信道，即使当用户没有数据要传送时，信道在用户时隙也是浪费的;也因为 CSMA/CD 是用户共享信道,所以当同时有用户需要使用信道时会发生碰撞，就降低信道的利用率，而 TDM 中用户在分配的时隙中不会与别的用户发生冲突。对局域网来说，连入信道的是相距较近的用户，因此通常信道带宽较宽，如果使用 TDM 方式，用户在自己的时隙内没有数据发送的情况会更多，不利于信道的充分利用。

对计算机通信来说，突发式的数据更不利于使用 TDM 方式。

3-20　假定 1km 长的 CSMA/CD 网络的数据率为 1Gb/s。设信号在网络上的传播速率为 200000km/s。求能够使用此协议的最短帧长。

答：对于 1km 电缆，单程传播时间为 1÷200000=5×10-6s，即 5us，来回路程传播时间为 10us。为了能够按照 CSMA/CD 工作，最短帧的发射时间不能小于 10us。以 1Gb/s 速率工作，10us 可以发送的比特数等于：

$$\frac{10\times10^{-6}}{1\times10^{-9}}=10000$$

因此，最短帧是 10000 位或 1250 字节长。

3-21　什么叫做比特时间？使用这种时间单位有什么好处？100 比特时间是多少微秒？

答：比特时间是指传输 1bit 所需要的时间。种时间单位与数据率密切相关，用它来计量时延可以将时间与数据量联系起来。

“比特时间”换算成“微秒”必须先知道数据率是多少。如数据率是 100Mb/s，则 100 比特时间等于 10us。

3-22 假定在使用 CSMA/CD 协议的 10Mb/s 以太网中某个站在发送数据时检测到碰撞，执行退避算法时选择了随机数 r=100.试问这个站需要等多长时间后才能再次发送数据？如果是 100Mb/s 的以太网呢？

答：对于 10Mb/s 的以太网，等待时间是 5.12 毫秒

对于 100Mb/s 的以太网，等待时间是 512 微妙。

3-23 公式（3-3）表示，以太网的极限信道利用率与链接在以太网上的站点数无关。能否由此推论出：以太网的利用率也与链接在以太网上的站点数无关？请说明理由。

答：实际的以太网各站发送数据的时刻是随机的，而以太网的极限信道利用率的得出是假定以太网使用了特殊的调度方法（已经不再是 CSMA/CD 了），使各站点的发送不发生碰撞。

3-24 假定站点 A 和 B 在同一个 10Mb/s 以太网网段上。这两个站点之间的时延为 225 比特时间。现假定 A 开始发送一帧，并且在 A 发送结束之前 B 也发送一帧。如果 A 发送的是以太网所容许的最短的帧，那么 A 在检测到和 B 发生碰撞之前能否把自己的数据发送完毕？换言之，如果 A 在发送完毕之前并没有检测到碰撞，那么能否肯定 A 所发送到帧不会和 B

发送的帧发生碰撞？（提示：在计算时应当考虑到每一个以太网帧在发送到信道上时，在MAC 帧前面还要增加若干字节的前同步码和帧定界符）

答：设在 t=0 时 A 开始发送。在 t=576 比特时间，A 应当发送完毕。

t=225 比特时间，B 就检测出 A 的信号。只要 B 在 t=224 比特时间之前发送数据，A 在发送完毕之前就一定检测到碰撞。就能够肯定以后也不会再发送碰撞了。

如果 A 在发送完毕之前并没有检测到碰撞，那么就能够肯定 A 所发送到帧不会和 B 发送的帧发生碰撞（当然也不会和其他的站点发送碰撞）。

3-25 在上题中的站点 A 和 B 在 t=0 时同时发送了数据帧。当 t=255 比特时间，A 和 B 同时检测到发送了碰撞，并且在 t=225+48=273 比特时间完成了干扰信号的传输。A 和 B 在 CSMA/CD 算法中选择不同的 r 值退避。假定 A 和 B 选择的随机数分别是 rA=0 和 rB=1.。试问 A 和 B 各在什么时间开始重传其数据帧？A 重传的数据帧在什么时间到达 B?A 重传的数据会不会和 B 重传的数据再次发送碰撞？B 会不会在预定的重传时间停止发送数据？

答：t=0 时，A 和 B 开始发送数据。

t=255 比特时间，A 和 B 都检测到碰撞。

t=273 比特时间，A 和 B 结束干扰信号的传输。

t=594 比特时间，A 开始发送

t=785 比特时间，B 再次检测信道。如空闲，则 B 在 881 比特时间发送数据。否则再退避。

A 重传的数据在 819 比特时间到达 B,B 先检测到信道忙，因此 B 在预定的 881 比特时间停止发送数据。

3-26 以太网上只有两个站，他们同时发送数据，产生了碰撞。于是按截断二进制指数退避算法进行重传。重传次数记为 i，i=1，2，3，。。。。试计算第一次重传失败的概率、第二次重传失败的概率、第三次重传失败的概率，以及一个站成功发送数据之前的平均重传次数 N。答：设第 i 次重传失败的概率为 Pi，显然

$$Pi=(0.5)^{k},\quad k=\min[i,10]$$

故第一次重传失败的概率 P1=0.5,

第二次重传失败的概率 P2=0.25,

第三次重传失败的概率 P3=0.125.。

P[传送 i 次才成功]=P[第 1 次传送失败]×P[第 2 次传送失败]×。。。×P[第 I -1 次传送失败]×P[第 i 次传送成功]

求 {P[传送 i 次才成功]}的统计平均值，得出平均重传次数为 1.637.

3-27 假定一个以太网上的通信量中的 80%是在本局域网上进行的，而且其余的 20%的通信量是在本局域网和因特网之间进行的。另一个以太网的情况则反过来。这两个以太网一个使用以太网集线器，而另一个使用以太网交换机。你认为以太网交换机应当用在哪一个网络上？

答：以太网交换机用在这样的以太网，其 20%通信量在本局域网内，而 80%的通信量到因特网。

3-28 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带宽。

（1）10 个站点连接到一个 10Mbit/s 以太网集线器；

（2）10 站点连接到一个 100Mbit/s 以太网集线器；

（3）10 个站点连接到一个 10Mbit/s 以太网交换机。

答：（1）10 个站共享 10Mbit/s；
（2）10 个站共享 100Mbit/s；
（3）每一个站独占 10Mbit/s。

3-29 10Mbit/s 以太网升级到 100Mbit/s 和 1Gbit/s 甚至 10Gbit/s 时，需要解决哪些技术问题？在帧的长度方面需要有什么改变？为什么？传输媒体应当有什么改变？

答：以太网升级时，由于数据传输率提高了，帧的发送时间会按比例缩短，这样会影响冲突的检测。所以需要减小最大电缆长度或增大帧的最小长度，使参数 a 保持为较小的值，才能有效地检测冲突。在帧的长度方面，几种以太网都采用 802.3 标准规定的以太网最小最大帧长，使不同速率的以太网之间可方便地通信。100bit/s 的以太网采用保持最短帧长（64byte）不变的方法，而将一个网段的最大电缆长度减小到 100m，同时将帧间间隔时间由原来的 9.6μs，改为 0.96μs。1Gbit/s 以太网采用保持网段的最大长度为 100m 的方法，用“载波延伸”和“分组突法”的办法使最短帧仍为 64 字节，同时将争用字节增大为 512 字节。传输媒体方面，10Mbit/s 以太网支持同轴电缆、双绞线和光纤，而 100Mbit/s 和 1Gbit/s 以太网支持双绞线和光纤，10Gbit/s 以太网只支持光纤。

3-30 以太网交换机有何特点？它与集线器有何区别？

答：以太网交换机实质上是一个多端口网桥。工作在数据链路层。以太网交换机的每个端口都直接与一个单个主机或另一个集线器相连，并且一般工作在全双工方式。交换机能同时连通许多对的端口，使每一对相互通信的主机都能像独占通信媒体一样，进行无碰撞地传输数据。通信完成后就断开连接。

区别：以太网交换机工作数据链路层，集线器工作在物理层。集线器只对端口上进来的比特流进行复制转发，不能支持多端口的并发连接。

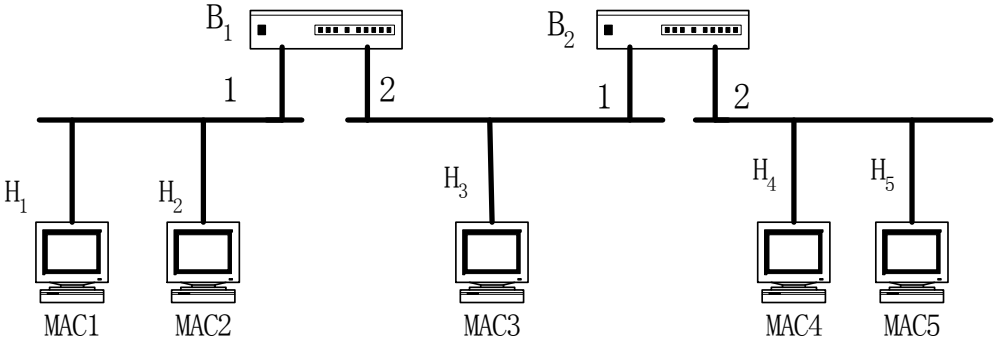
3-31 网桥的工作原理和特点是什么？网桥与转发器以及以太网交换机有何异同？

答：网桥的每个端口与一个网段相连，网桥从端口接收网段上传送的各种帧。每当收到一个帧时，就先暂存在其缓冲中。若此帧未出现差错，且欲发往的目的站 MAC 地址属于另一网段，则通过查找站表，将收到的帧送往对应的端口转发出去。若该帧出现差错，则丢弃此帧。网桥过滤了通信量，扩大了物理范围，提高了可靠性，可互连不同物理层、不同 MAC 子层和不同速率的局域网。但同时也增加了时延，对用户太多和通信量太大的局域网不适合。

网桥与转发器不同，（1）网桥工作在数据链路层，而转发器工作在物理层；（2）网桥不像转发器转发所有的帧，而是只转发未出现差错，且目的站属于另一网络的帧或广播帧；（3）转发器转发一帧时不用检测传输媒体，而网桥在转发一帧前必须执行 CSMA/CD 算法；（4）网桥和转发器都有扩展局域网的作用，但网桥还能提高局域网的效率并连接不同 MAC 子层和不同速率局域网的作用。

以太网交换机通常有十几个端口，而网桥一般只有 2-4 个端口；它们都工作在数据链路层；网桥的端口一般连接到局域网，而以太网的每个接口都直接与主机相连，交换机允许多对计算机间能同时通信，而网桥允许每个网段上的计算机同时通信。所以实质上以太网交换机是一个多端口的网桥，连到交换机上的每台计算机就像连到网桥的一个局域网段上。网桥采用存储转发方式进行转发，而以太网交换机还可采用直通方式转发。以太网交换机采用了专用的交换机构芯片，转发速度比网桥快。

3-32 现有五个站分别连接在三个局域网上，并且用两个透明网桥连接起来，如下图所示。每一个网桥的两个端口号都标明在图上。在一开始，两个网桥中的转发表都是空的。以后有以下各站向其他的站发送了数据帧，即 H1 发送给 H5，H3 发送给 H2，H4 发送给 H3，H2 发送给 H1。试将有关数据填写在下表中



答：

发送的帧	网桥 1 的转发表		网桥 2 的转发表		网桥 1 的处理（转发？丢弃？登记？）	网桥 2 的处理（转发？丢弃？登记？）
	站地址	端口	站地址	端口		
H1→H5	MAC1	1	MAC1	1	转发，写入转发表	转发，写入转发表
H3→H2	MAC3	2	MAC3	1	转发，写入转发表	转发，写入转发表
H4→H3	MAC4	2	MAC4	2	写入转发表，丢弃不转发	转发，写入转发表
H2→H1	MAC2	1			写入转发表，丢弃不转发	接收不到这个帧

3-33 网桥中的转发是用自学习算法建立的。如果有的站点总是不发送数据而仅仅接收数据，那么在转发表中是否就没有与这样的站点相对应的项目？如果要向这个站点发送数据帧，那么网桥能够把数据帧正确转发到目的地址吗？

答：如果站点仅仅接受数据那么在转发表中就没有这样的项目。网桥能把数据帧正确的发送到目的地址。如果不知道目的地地址的位置，源机器就发布一广播帧，询问它在哪里。每个网桥都转发该查找帧(discovery frame)，这样该帧就可到达互联网中的每一个 LAN。当答复回来时，途经的网桥将它们自己的标识记录在答复帧中，于是，广播帧的发送者就可以得到确切的路由，并可从中选取最佳路由。

第 4 章 网络层

4-01 网络层向上提供的服务有哪两种？试比较其优缺点。

答案：虚电路服务和数据报服务。

虚电路的优点：虚电路服务是面向连接的，网络能够保证分组总是按照发送顺序到达目的站，且不丢失、不重复，提供可靠的端到端数据传输；目的站地址仅在连接建立阶段使用，每个分组使用短的虚电路号，使分组的控制信息部分的比特数减少，减少了额外开销；端到端的差错处理和流量控制可以由分组交换网负责，也可以由用户机负责。虚电路服务适用于通信信息量大、速率要求高、传输可靠性要求高的场合。

虚电路的缺点：虚电路服务必须建立连接；属于同一条虚电路的分组总是按照同一路由进行转发；当结点发生故障时，所有通过出故障的结点的虚电路均不能工作。

数据报的优点：数据报服务不需要建立连接；每个分组独立选择路由进行转发，当某个结点发生故障时，后续的分组可以另选路由，因而提高了通信的可靠性。数据报服务的灵活性好，适用于传输可靠性要求不高、通信子网负载不均衡、需要选择最佳路径的场合。

数据报的缺点：数据报服务是面向无连接的，到达目的站时不一定按发送顺序，传输中的分组可能丢失和重复，提供面向无连接的、不可靠的数据传输；每个分组都要有目的站的全地址；当网络发生故障是，出故障的结点可能会丢失数据，一些路由可能会发生变化；端到端的差错处理和流量控制只由主机负责。

4-02 网络互连有何实际意义？进行网络互连时，有哪些共同的问题需要解决？

答案：网络互连暗含了相互连接的计算机进行通信，也就是说从功能上和逻辑上看，这些相互连接的计算机网络组成了一个大型的计算机网络。网络互连可以使处于不同地理位置的计算机进行通信，方便了信息交流，促成了当今的信息世界。

存在问题有：不同的寻址方案；不同的最大分组长度；不同的网络介入机制；不同的超时控制；不同的差错恢复方法；不同的状态报告方法；不同的路由选择技术；不同的用户接入控制；不同的服务（面向连接服务和无连接服务）；不同的管理与控制方式；等等。

注：网络互连使不同结构的网络、不同类型的机器之间互相连通，实现更大范围和更广泛意义上的资源共享。

4-03 作为中间系统，转发器、网桥、路由器和网关都有何区别？

答案：

1）转发器、网桥、路由器、和网关所在的层次不同。

转发器是物理层的中继系统。

网桥是数据链路层的中继系统。

路由器是网络层的中继系统。

在网络层以上的中继系统为网关。

2）当中继系统是转发器或网桥时，一般并不称之为网络互连，因为仍然是一个网络。

路由器其实是一台专用计算机，用来在互连网中进行路由选择。一般讨论的互连网都是指用路由器进行互连的互连网络。

4-04 试简单说明 IP、ARP、RARP 和 ICMP 协议的作用。

答：IP:网际协议，它是 TCP/IP 体系中两个最重要的协议之一，IP 使互连起来的许多计算机网络能够进行通信。无连接的数据报传输. 数据报路由。

ARP（地址解析协议），实现地址转换：将 IP 地址转换成物理地址。

RARP（逆向地址解析协议）， 将物理地址转换成 IP 地址。

ICMP:Internet 控制消息协议，进行差错控制和传输控制，减少分组的丢失。

注：ICMP 协议帮助主机完成某些网络参数测试，允许主机或路由器报告差错和提供有关异常情况报告，但它没有办法减少分组丢失，这是高层协议应该完成的事情。IP 协议只是尽最大可能交付，至于交付是否成功，它自己无法控制。

4-05 IP 地址分为几类？各如何表示？ IP 地址的主要特点是什么？

答案：目前的 IP 地址（IPv4：IP 第四版本）由 32 个二进制位表示，每 8 位二进制数为一个整数，中间由小数点间隔，如 159.226.41.98，整个 IP 地址空间有 4 组 8 位二进制数，表示主机所在网络的地址（类似部队的编号）以及主机在该网络中的标识（如同士兵在该部队的编号）共同组成。

为了便于寻址和层次化的构造网络，IP 地址被分为 A、B、C、D、E 五类，商业应用中只用到 A、B、C 三类。

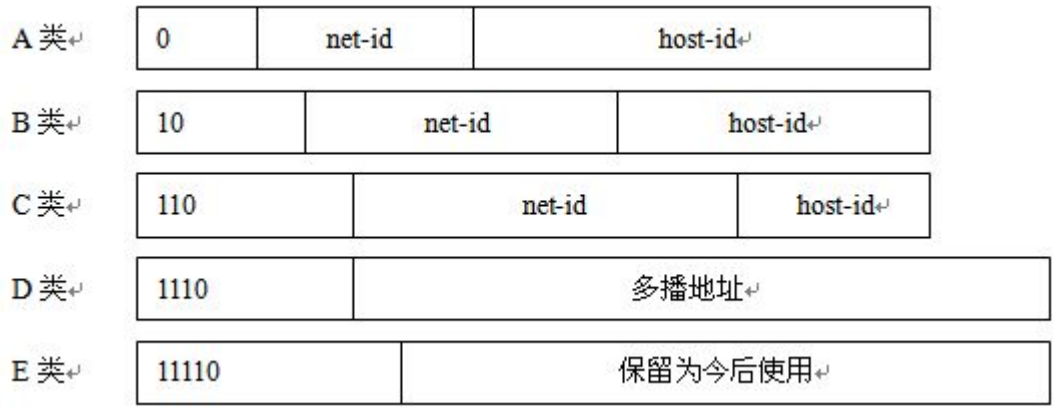
A 类地址：A 类地址的网络标识由第一组 8 位二进制数表示，网络中的主机标识占 3 组 8 位二进制数，A 类地址的特点是网络标识的第一位二进制数取值必须为“0”。不难算出，A 类地址允许有 126 个网段，每个网络大约允许有 1 670 万台主机，通常分配给拥有大量主机的网络（如主干网）。

B 类地址：B 类地址的网络标识由前两组 8 位二进制数表示，网络中的主机标识占两组 8 位二进制数，B 类地址的特点是网络标识的前两位二进制数取值必须为“10”。B 类地址允许有 16 384 个网段，每个网络允许有 65 533 台主机，适用于结点比较多的网络 (如区域网)。

C 类地址：C 类地址的网络标识由前 3 组 8 位二进制数表示，网络中的主机标识占 1 组 8 位二进制数，C 类地址的特点是网络标识的前 3 位二进制数取值必须为“110”。具有 C 类地址的网络允许有 254 台主机，使用于结点比较少的网络（如校园网）。

为了便于记忆，通常习惯采用 4 个十进制数来表示一个 IP 地址，十进制数之间采用句点“.”予以分隔。这种 IP 地址的表示方法也被陈伟点分十进制法。如以这种方式表示，A 类网络的 IP 地址范围为 1.0.0.1-127.255.255.254；B 类网络的 IP 地址范围为：128.1.0.1-191.255.255.254；C 类网络的 IP 地址范围为：192.0.1.1-223.255.255.254.

IP 地址共分 5 类，分类情况如题 4-05 解图所示：



题 4-05 解图

IP 地址是 32 位地址，其中分为 netid（网络号），和 hostid（主机号）。特点如下：

1.IP 地址不能反映任何有关主机位置的物理信息；

2.一个主机同时连接在多个网络上时，该主机就必须有多个 IP 地址；

3.由转发器或网桥连接起来的若干个局域网仍为一个网络；

4.所有分配到网络号（netid）的网络都是平等的；

5.IP 地址可用来指明一个网络的地址。

4-06 试根据 IP 地址的规定，计算出表 4-2 中的数据。

表 4-2　IP 地址的指派范围

网络类型	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中的最大主机数
A	126（2^7-2）	1	126	16777214
B	16383（2^{14}-1）	128.1	191.255	65534
C	2097151（2^{21}-1）	192.0.1	233.255.255	254

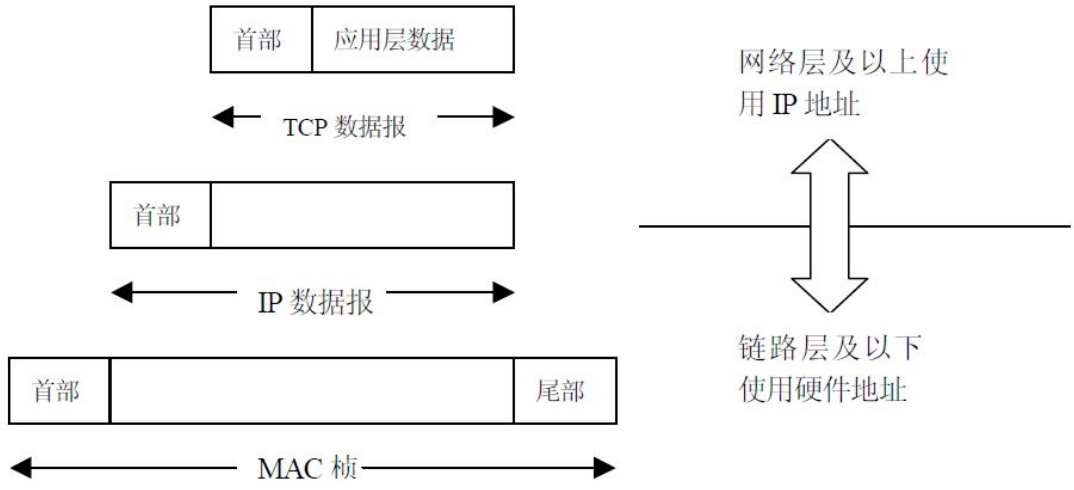
答案：1）A 类网中，网络号占七个 bit，则允许用的网络数为 2 的 7 次方，为 128，但是要除去 0 和 127 的情况，所以能用的最大网络数是 126，第一个网络号是 1，最后一个网络号是 126。主机号占 24 个 bit，则允许用的最大主机数为 2 的 24 次方，为 16777216，但是也要除去全 0 和全 1 的情况，所以能用的最大主机数是 16777214。

2） B 类网中，网络号占 14 个 bit，则能用的最大网络数为 2 的 14 次方，为 16384，第一个网络号是 128.0，因为 127 要用作本地软件回送测试，所以从 128 开始，其点后的还可以容纳 2 的 8 次方为 256，所以以 128 为开始的网络号为 128.0~~128.255，共 256 个，以此类推，第 16384 个网络号的计算方法是：16384/256=64128+64=192，则可推算出为 191.255。主机号占 16 个 bit，则允许用的最大主机数为 2 的 16 次方，为 65536，但是也要除去全 0 和全 1 的情况，所以能用的最大主机数是 65534。

3）C 类网中，网络号占 21 个 bit，则能用的网络数为 2 的 21 次方，为 2097152，第一个网络号是 192.0.0，各个点后的数占一个字节，所以以 192 为开始的网络号为 192.0.0~~192.255.255，共 256×256=65536，以此类推，第 2097152 个网络号的计算方法是：2097152/65536=32192+32=224，则可推算出为 223.255.255。主机号占 8 个 bit，则允许用的最大主机数为 2 的 8 次方，为 256，但是也要除去全 0 和全 1 的情况，所以能用的最大主机数是 254。

4-07 试说明 IP 地址与硬件地址的区别。为什么要使用这两种不同的地址？

答案：如图所示，IP 地址在 IP 数据报的首部，而硬件地址则放在 MAC 帧的首部。在网络层以上使用的是 IP 地址，而链路层及以下使用的是硬件地址。



题 4-07 图解

在 IP 层抽象的互连网上，我们看到的只是 IP 数据报，路由器根据目的站的 IP 地址进行选路。在具体的物理网络的链路层，我们看到的只是 MAC 帧，IP 数据报被封装在 MAC 帧里面。MAC 帧在不同的网络上传送时，其 MAC 帧的首部是不同的。这种变化，在上面的 IP 层上是看不到的。每个路由器都有 IP 地址和硬件地址。使用 IP 地址与硬件地址，尽管连接在一起的网络的硬件地址体系各不相同，但 IP 层抽象的互连网却屏蔽了下层这些很复杂的细节，并使我们能够使用统一的、抽象的 IP 地址进行通信。

4-08 IP 地址方案与我国的电话号码体制的主要不同点是什么？

答案：IP 地址分为网络号和主机号，它不反映有关主机地理位置的信息。而电话号码反映有关电话的地理位置的信息，同一地域的电话号码相似。

注：我国电话号码体制是按照行政区域划分的层次结构，同一地域的电话号码有相同的若干位前缀。号码相近的若干话机，其地理位置应该相距较近。IP 地址没有此属性，其网络号和主机地理位置没有关系。

4-09（1）子网掩码为 255.255.255.0 代表什么意思？

（2）一网络的现在掩码为 255.255.255.248，问该网络能够连接多少个主机？

（3）一 A 类网络和一 B 类网络的子网号 subnet-id 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？

（4）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？

（5）一 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？

（6）某个 IP 地址的十六进制表示为 C2.2F.14.81，试将其转换为点分十进制的形式。这个地址是哪一类 IP 地址？

（7）C 类网络使用子网掩码有无实际意义？为什么？

答案：（1）可以代表 C 类地址对应的子网掩码默认值；也能表示 A 类和 B 类地址的掩码,前 24 位决定网络号和子网号，后 8 位决定主机号。（用 24bit 表示网络部分地址，包括网络号和子网号）

（2）255.255.255.248 化成二进制序列为：11111111 11111111 11111111 11111000，根据掩码的定义，后三位是主机号，一共可以表示 8 个主机号，除掉全 0 和全 1 的两个，该网络能够接 6 个主机。

（3）子网掩码的形式是一样的，都是 255.255.255.0；但是子网的数目不一样，前者为 65534，后者为 254。

（4）255.255.240.0（11111111.11111111.11110000.00000000）是 B 类地址的子网掩码，主机地址域为 12 比特，所以每个子网的主机数最多为：2^{12}-2=4 094。

（5）子网掩码由一连串的 1 和一连串的 0 组成，1 代表网络号和子网号，0 对应主机号.255.255.0.255 变成二进制形式是：11111111 11111111 00000000 11111111.可见，是一个有效的子网掩码，但是不是一个方便使用的解决办法。

（6）用点分十进制表示，该 IP 地址是 194.47.20.129，为 C 类地址。

（7）有，可以提高网络利用率。

注：实际环境中可能存在将 C 类网网络地址进一步划分为子网的情况，需要掩码说明子网号的划分。C 类网参加互连网的路由，也应该使用子网掩码进行统一的 IP 路由运算。C 类网的子网掩码是 255.255.255.0。

4-10 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

答案：(1) 128.36.199.3　　B 类网

(2) 21.12.240.17　　A 类网

(3) 183.194.76.253　　B 类网

(4) 192.12.69.248　　C 类网

(5) 89.3.0.1　　A 类网

(6) 200.3.6.2　　C 类网

4-11 IP 数据报中的首部检验和并不检验数据报中的数据。这样做的最大好处是什么？坏处是什么？

答案：好处是数据报每经过一个结点，结点只检查首部的检验和，使结点工作量降低，网络速度加快。

坏处是只检验首部，不包括数据部分，即使数据出错也无法得知，只有到目的主机才能发现。

4-12 当某个路由器发现一 IP 数据报的检验和有差错时，为什么采取丢弃的办法而不是要求源站重传此数据报？计算首部检验和为什么不采用 CRC 检验码？

答案：之所以不要求源站重发，是因为地址子段也有可能出错，从而找不到正确的源站。

数据报每经过一个结点，结点处理机就要计算一下校验和。不用 CRC，就是为了简化计算。

4-13.设 IP 数据报使用固定首部，其各字段的具体数值如图所示（除 IP 地址外，均为十进制表示）。试用二进制运算方法计算应当写入到首部检验和字段中的数值（用二进制表示）。

4　　5　　0　　28

1　　0　　0

4　　17

10.12.14.5

12.6.7.9

1000101　00000000　00000000-00011100

00000000　00000001　00000000-00000000

00000100　00010001　xxxxxxxx　xxxxxxxx

00001010　00001100　00001110　00000101

00001100　00000110　00000111　00001001　作二进制检验和（XOR）

01110100　01001110 取反码

10001011　10110001

4-14. 重新计算上题，但使用十六进制运算方法（没 16 位二进制数字转换为 4 个十六进制数字，再按十六进制加法规则计算）。比较这两种方法。

01000101 00000000 00000000-00011100 4 5 0 0 0 0 1 C
00000000 00000001 00000000-00000000 0 0 0 1 0 0 0 0
00000100 000010001 xxxxxxxx xxxxxxxx 0 4 1 1 0 0 0 0
00001010 00001100 00001110 00000101 0 A 0 C 0 E 0 5
00001100 00000110 00000111 00001001 0 C 0 6 0 7 0 9
01011111 00100100 00010101 00101010 5 F 2 4 1 5 2 A
5 F 2 4
1 5 2 A

---

7 4 4 E-→8 B B 1

4-15.什么是最大传送单元 MTU？它和 IP 数据报的首部中的哪个字段有关系？

答：IP 层下面数据链里层所限定的帧格式中数据字段的最大长度，与 IP 数据报首部中的总长度字段有关系

4-16 在因特网中将 IP 数据报分片传送的数据报在最后的目的主机进行组装。还可以有另一种做法，即数据报片通过一个网络就进行一次组装。试比较这两种方法的优劣。

答案：前一种方法对于所传数据报来将仅需要进行一次分段一次组装，用于分段和组装的开销相对较小。

但主机若在最终组装时发现分组丢失，则整个数据报要重新传输，时间开销很大。

后一种方法分段和组装的次数要由各个网络所允许的最大数据报长度来决定，分段和组装的开销相对较大。但若通过一个网络后组装时发现分段丢失，可以及时地重传数据报，时间开销较前者小，同时可靠性提高。

4-17 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比特的数据（这里的“数据”当然指的是局域网看见的数据）？

答案：IP 数据报的长为：3200+160=3360 bit

第二个局域网分片应分为 [3200/1200]=3 片。

三片的首部共为：160*3=480 bit

则总共要传送的数据共 3200+480=3680 bit。

4-18（1）有人认为：“ARP 协议向网络层提供了转换地址的服务，因此 ARP 应当属于数据链路层。”这种说法为什么是错误的？

（2）试解释为什么 ARP 高速缓存每存入一个项目就要设置 10~20 分钟的超时计时器。这个时间设置得太大或太小会出现什么问题？

（3）至少举出两种不需要发送 ARP 请求分组的情况（即不需要请求将某个项目的 IP 地址解析为相应的硬件地址）。

答案：（1）ARP 不是向网络层提供服务，它本身就是网络层的一部分，帮助向传输层提供服务。在数据链路层不存在 IP 地址的问题。数据链路层协议是像 HDLC 和 PPP 这样的协议，它们把比特串从线路的一端传送到另一端。

（2）ARP 将保存在高速缓存中的每一个映射地址项目都设置生存时间（例如，10~20 分钟）。凡超过生存时间的项目就从高速缓存中删除掉。设置这种地址映射项目的生存时间是很重要的。设想有一种情况，主机 A 和 B 通信，A 的 ARP 高速缓存里保存有 B 的物理地址，

但 B 的网卡突然坏了，B 立即更换了一块，因此 B 的硬件地址就改变了。A 还要和 B 继续通信。A 在其 ARP 高速缓存中查找到 B 原先的硬件地址，并使用该硬件地址向 B 发送数据帧，但 B 原先的硬件地址已经失效了，因此 A 无法找到主机 B。是过了一段时间，A 的 ARP 高速缓存中已经删除了 B 原先的硬件地址（因为它的生存时间到了），于是 A 重新广播发送 ARP 请求分组，又找到了 B。

时间设置太大，造成 A 一直空等而产生通讯时延，网络传输缓慢。若太小，有可能网络状况不好，B 暂时没有应答 A，但 A 已经认为 B 的地址失效，A 重新发送 ARP 请求分组，造成通讯时延。

（3）主机 A 和 B 通讯，A 的 ARP 高速缓存里保存有 B 的物理地址，此时不需要发送 ARP 请求分组。

当主机 A 向 B 发送数据报时，很可能不久以后主机 B 还要向 A 发送数据报，因而主机 B 也可能要向 A 发送 ARP 请求分组。为了减少网络上的通信量，主机 A 在发送其 ARP 请求分组时，就将自己 IP 地址到硬件的映射写入 ARP 请求分组。当主机 B 收到 A 的 ARP 请求分组时，就将主机 A 的这一地址映射写入主机 B 自己的 ARP 高速缓存中。这对主机 B 以后向 A 发送数据报时就更方便了。

4-19. 主机 A 发送 IP 数据报给主机 B,途中经过了 5 个路由器。试问在 IP 数据报的发送过程总共使用几次 ARP?

解：前提，理论上当前主机路由器 arp 表中都没有下一跳路由器 MAC 共需 6 次,主机 A 先通过 arp 得到第一个路由器的 MAC,之后每一个路由器转发前都通过 ARP 得到下一跳路由器的 MAC，最后一条路由器将 IP 包发给 B 前仍要通过 ARP 得到 B 的 MAC，共 6 次。

4-20. 设某路由器建立了如下路由表（这三列分别是目的网络、子网掩码和下一跳路由器，若直接交付则最后一列表示应当从哪一个接口转发出去）：

目的网络　　子网掩码　　下一跳

128.96.39.0　　255.255.255.128　　接口 0

128.96.39.128　　255.255.255.128　　接口 1

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，其目的站 IP 地址分别为：

（1）128.96.39.10

（2）128.96.40.12

（3）128.96.40.151

（4）192.4.153.17

（5）192.4.153.90

试分别计算其下一跳。

解：（1）分组的目的站 IP 地址为：128.96.39.10。先与子网掩码 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。

4-21 某单位分配到一个 B 类 IP 地址，其 net-id 为 129.250.0.0。该单位有 4000 台机器，平均分布在 16 个不同的地点。如选用子网掩码为 255.255.255.0，试给每一地点分配一个子网号码，并计算出每个地点主机号码的最小值和最大值。

答：4000/16=250，平均每个地点 250 台机器。如选 255.255.255.0 为掩码，则每个网络所连主机数=28-2=254>250，共有子网数=28-2=254>16，能满足实际需求。

可给每个地点分配如下子网号码

地点： 子网号（subnet-id） 子网网络号 主机 IP 的最小值和最大值

1： 00000001 129.250.1.0 129.250.1.1---129.250.1.254

2： 00000010 129.250.2.0 129.250.2.1---129.250.2.254

3： 00000011 129.250.3.0 129.250.3.1---129.250.3.254

4： 00000100 129.250.4.0 129.250.4.1---129.250.4.254

5： 00000101 129.250.5.0 129.250.5.1---129.250.5.254

6： 00000110 129.250.6.0 129.250.6.1---129.250.6.254

7： 00000111 129.250.7.0 129.250.7.1---129.250.7.254

8： 00001000 129.250.8.0 129.250.8.1---129.250.8.254

9： 00001001 129.250.9.0 129.250.9.1---129.250.9.254

10： 00001010 129.250.10.0 129.250.10.1---129.250.10.254

11： 00001011 129.250.11.0 129.250.11.1---129.250.

11.254

12： 00001100 129.250.12.0 129.250.12.1---129.250.12.254

13： 00001101 129.250.13.0 129.250.13.1---129.250.13.254

14： 00001110 129.250.14.0 129.250.14.1---129.250.14.254

15： 00001111 129.250.15.0 129.250.15.1---129.250.15.254

16： 00010000 129.250.16.0 129.250.16.1---129.250.16.254

4-22 一具数据报长度为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

4-23 分两种情况（使用子网掩码和使用CIDR）写出因特网的IP层查找路由的算法。

答：见课本P134、P139

4-24 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）20，（4）62，（5）122，（6）250

答：（3）20+2=22<25（加2即将不能作为子网号的全1和全0的两种，所以子网号占用5bit，所以网络号加子网号共13bit，子网掩码为前13个1后19个0，即255.248.0.0。依此方法：

（1）255.192.0.0，（2）255.224.0.0，（4）255.252.0.0，（5）255.254.0.0，（6）255.255.0.0

4-25 以下有四个子网掩码，哪些是不推荐使用的？为什么？

（1）176.0.0.0，（2）96.0.0.0，（3）127.192.0.0，（4）255.128.0.0

答：只有（4）是连续的1和连续的0的掩码，是推荐使用的。

4-26 有如下的四个/24地址块，试进行最大可能的聚合。

212.56.132.0/24

212.56.133.0/24

212.56.134.0/24

212.56.135.0/24

答：212=（11010100）2，56=（00111000）2

132=（10000100）2，

133=（10000101）2

134=（10000110）2，

135=（10000111）2

所以共同的前缀有 22 位，即 11010100 00111000 100001，聚合的 CIDR 地址块是：212.56.132.0/22

4-27 有两个 CIDR 地址块 208.128/11 和 208.130.28/22。是否有哪一个地址块包含了另一地址块？如果有，请指出，并说明理由。

答：208.128/11 的前缀为：11010000 100

208.130.28/22 的前缀为：11010000 10000010 000101，它的前 11 位与 208.128/11 的前缀是一致的，所以 208.128/11 地址块包含了 208.130.28/22 这一地址块。

4-28 已知路由器 R1 的路由表如表 4-12 所示。

表 4-12　习题 4-28 中的路由器 R1 的路由表

地址掩码	目的网络地址	下一跳地址	路由器接口
/26	140.5.12.64	180.15.2.5	M2
/24	130.5.8.0	190.16.6.2	M1
/16	110.71.0.0	----	M0
/16	180.15.0.0	----	M2
/16	190.16.0.0	----	M1
默认	默认	110.71.4.5	M0

试画出各网络和必要的路由器的连接拓扑，标注出必要的 IP 地址和接口。对不能确定的情况应当指明。

答案：图形见课后答案 P380

4-29 一个自治系统有 5 个局域网，其连接图如图 4-55 示。LAN_2 至 LAN_5 上的主机数分别为：91，150，3 和 15.该自治系统分配到的 IP 地址块为 30.138.118/23.试给出每一个局域网的地址块（包括前缀）。

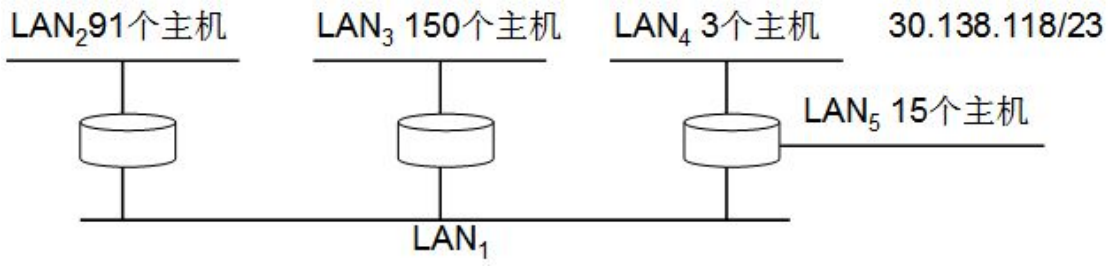


图 4-55　习题 4-29 的图

答案：对 LAN_3，主机数 150，（2^7-2）<150+1<（2^8-2），所以主机位为 8bit，网络前缀为 24，分配地址块 30.138.118.0/24。（第 24 位为 0）

对 LAN_2，主机数 91，（2^6-2）<91+1<（2^7-2），所以主机位为 7bit，网络前缀为 25，分配地址块 30.138.119.0/25。（第 24、25 位为 10）

对 LAN_5，主机数 15，（2^4-2）<15+1<（2^5-2），所以主机位为 5bit，网络前缀为 27，分配地址块 30.138.119.192/27。（第 24、25、26、27 位为 1110）

对 LAN_1，主机数 3，（2^2-2）<3+1<（2^3-2），所以主机位为 3bit，网络前缀为 29，分配地址块 30.138.119.232/29。（第 24、25、26、27、28、29 位为 111101）

对 LAN_4，主机数 3，（2^2-2）<3+1<（2^3-2），所以主机位为 3bit，网络前缀为 29，分配地址块 30.138.119.240/29。（第 24、25、26、27、28、29 位为 111110）

4-30 一个大公司有一个总部和三个下属部门。公司分配到的网络前缀是 192.77.33/24。公司的网络布局如图 4-56。总部共有五个局域网，其中 LAN_1～LAN_4 都连接到路由器 R_1 上，R_1 再通过 LAN_5 与路由其 R_5 相连。R_6 和远地的三个部门的局域网 LAN_6～LAN_8 通过广域网相连。每个局域网旁边标明的数字是局域网上主机数。试给每个局域网分配一个合适的网络前缀。

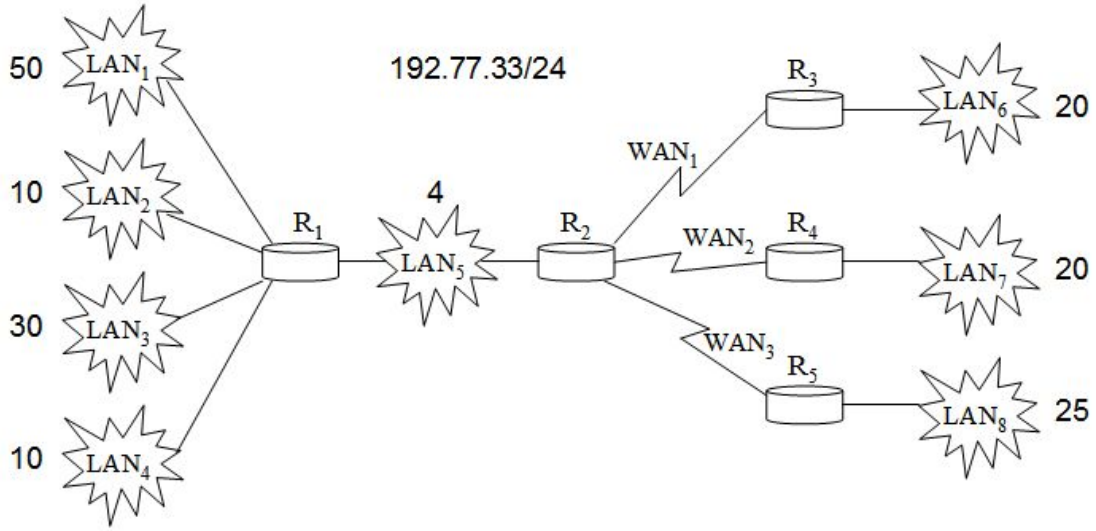


图 4-56　习题 4-30 的图

答案：分配网络前缀时应先分配地址数较多的前缀，本题的答案很多种，下面是其中的一种答案.

LAN1：192.77.33.0/26

LAN3：192.77.33.64/27；

LAN6：192.77.33.192/27；

LAN7：192.77.33.160/27；

LAN8；192.77.33.128/27

LAN2：192.77.33.96/28；

LAN4：192.77.33.11228

LAN5：192.77.33.224/27（考虑到以太网可能还要连接及个主机，故留有余地)WAN1:192.77.33.232/30；WAN2：192.77.33.236/30；192.77.33.240/30

4-31 以下地址中的哪一个和 86.32/12 匹配？请说明理由。

（1）86.33.224.123；（2）86.79.65.216；（3）86.58.119.74；（4）86.68.206.154。

答案：

（1）与 11111111 11110000 00000000 00000000 逐比特相“与”和 86.32/12 匹配

（2）与 11111111 11110000 00000000 00000000 逐比特相“与”和 86.32/12 不匹配

（3）与 11111111 11110000 00000000 00000000 逐比特相“与”和 86.32/12 不匹配

（4）与 11111111 11110000 00000000 00000000 逐比特相“与”和 86.32/12 不匹配

4-32 以下的地址前缀中哪一个地址和 2.52.90.140 匹配？请说明理由。

（1）0/4；（2）32/4；（3）4/6；（4）80/4。

答案：（1）2.52.90.140 与 11110000 00000000 00000000 00000000 逐比特相“与”和 0/4 匹配

（2）2.52.90.140 与 11110000 00000000 00000000 00000000 逐比特相“与”和 32/4 不匹配

（3）2.52.90.140 与 11110000 00000000 00000000 00000000 逐比特相“与”和 4/6 不匹配

（4）2.52.90.140 与 11110000 00000000 00000000 00000000 逐比特相“与”和 80/4 不匹配

4-33 下面的前缀中的哪一个和地址 152.7.77.159 及 152.31.47.252 都匹配？请说明理由。

（1）152.40/13；（2）153.40/9；（3）152.64/12；（4）152.0/11。

答案：（1）152.7.77.159 与 11111111 11111000 00000000 00000000 逐比特相“与”和（1）不匹配，故（1）不符合条件。

（1）152.7.77.159 与 11111111 10000000 00000000 00000000 逐比特相“与”和（2）不匹配，故（2）不符合条件。

（1）152.7.77.159 与 11111111 11110000 00000000 00000000 逐比特相“与”和（3）不匹配，故（3）不符合条件。

（1）152.7.77.159 与 11111111 11100000 00000000 00000000 逐比特相“与”和（4）匹配，152.31.47.252 和 11111111 11100000 00000000 00000000 逐比特相“与”和（4）匹配，故（4）不符合条件。

4-34 与下列掩码相对应的网络前缀各有多少比特？

（1）192.0.0.0；（2）240.0.0.0；（3）255.224.0.0；（4）255.255.255.252。

答案：点分十进制的地址化成二进制记法，1 的个数就是前缀的个数。

（1）11000000 00000000 00000000 00000000，对应的网络前缀是 2 比特

（2）11110000 00000000 00000000 00000000，对应的网络前缀是 4 比特

（3）11111111 11100000 00000000 00000000，对应的网络前缀是 11 比特

（4）11111111 11111111 11111111 11111100，对应的网络前缀是 30 比特

4-35. 已知地址块中的一个地址是 140.120.84.24/20。试求这个地址块中的最小地址和最大地址。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？

140.120.84.24 ➔ 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.相当于 16 个 C 类地址。

4-36.已知地址块中的一个地址是 190.87.140.202/29。重新计算上题。

190.87.140.202/29 ➔ 190.87.140.(1100 1010)/29

最小地址是 190.87.140.(1100 1000)/29 200

最大地址是 190.87.140.(1100 1111)/29 207

地址数是 8.相当于 1/32 个 C 类地址。

4-37 某单位分配到一个地址块 136.23.12.64/26。现在需要进一步划分 4 个一样大的子网。试问：

（1）每个子网的前缀有多长？

（2）每一个子网中有多少个地址？

（3）每一个子网的地址块是什么？

（4）每一个子网可分配给主机使用的最小地址和最大地址是什么？

4-38 IGP 和 EGP 这两类协议的主要区别是什么？

答案：IGP：内部网关协议，只关心本自治系统内如何传送数据报，与互联网中其他自治系统使用说明协议无关。

EGP：外部网关协议，在不同的 AS 边界传递路由信息的协议，不关心 AS 内部使用何种协议。

4-39 试简述 RIP、OSPF 和 BGP 路由选择协议的主要特点。

答案：

主要特点	RIP	OSPF	BGP
网关协议	内部	外部	外部
路由表内容	目的网，下一站，距离	目的网，下一站，距离	目的网，完美路由
最优通路依据	跳数	费用	多种策略
算法	距离矢量	链路状态	距离矢量
传送方式	运输层 UDP	IP 数据报	建立 TCP 连接
其他	简单； 效率低； 跳数为 16，不可达； 好消息传的快，坏消息传的慢	效率高； 路由器频繁交换信息， 难维持一致性； 规模大，统一度量，可达性	

4-40 RIP 使用 UDP，OSPF 使用 IP，而 BGP 使用 TCP。这样做有何优点？为什么 RIP 周期性地和临站交换路由信息而 BGP 却不这样做？

答案：RIP 协议处于 UDP 协议的上层，RIP 所接收的路由信息都封装在 UDP 的数据报中；OSPF 的位置位于网络层，由于要交换的信息量较大，故应使报文的长度尽量短，故采用 IP；BGP 要在不同的自治系统之间交换路由信息，由于网络环境复杂，需要保证可靠的传输，所以选择 TCP。

内部网关协议主要是设法使数据报载一个自治系统中尽可能有效地从源站传送到目的站，在一个自治系统内部并不需要考虑其他方面的策略，然而 BGP 使用的环境却不同。主要有以下三个原因：第一，因特网规模太大，使得自治系统之间的路由选择非常困难。第二，对于自治系统之间的路由选择，要寻找最佳路由是不现实的。第三，自治系统之间的路由选择必须考虑有关策略。由于上述情况，边界网关协议 BGP 只能是力求寻找一条能够到达目的地网络且比较好的路由，而并非要寻找一条最佳路由，所以 BGP 不需要像 RIP 那样周期性和临站交换路由信息。，

4-41 假定网络中的路由器 B 的路由表有如下的项目（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	C
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”和“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）。

解：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

4-42 假定网络中的路由器 A 的路由表有如下的项目（这三列分别表示“目的网络”、“距离”和“下一跳路由器”）

N1	4	B
N2	2	C
N3	1	F
N4	5	G

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

N1	2
N2	1
N3	3

试求出路由器 A 更新后的路由表（详细说明每一个步骤）。

解：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，更新
N2	2	C	相同的下一跳，更新
N3	1	F	不同的下一跳，距离更长，不改变
N4	5	G	无新信息，不改变

4-43 IGMP 协议的要点是什么？隧道技术是怎样使用的？

答案：要点有：1、IGMP 是用来进行多播的，采用多播协议可以明显地减轻网络中的各种资源的消耗，IP 多播实际上只要硬件多播的一种抽象；2、IGMP 只有两种分组，即询问分组和响应分组。IGMP 使用 IP 数据报传递其报文，但它也向 IP 提供服务；3、IGMP 属于整个网际协议 IP 的一个组成部分，IGMP 也是 TCP/IP 的一个标准。

隧道技术使用：当多播数据报在传输过程中，若遇到不运行多播路由器的网络，路由器就对多播数据报进行再次封装（即加上一个普通数据报的首部，使之成为一个向单一目的站

发送的单播数据报），通过了隧道以后，再由路由器剥去其首部，使它又恢复成原来的多播数据报，继续向多个目的站转发

。

4-44 什么是 VPN？VPN 有什么特点和优缺点？VPN 有几种类别？

答案：P171-173

4-45 什么是 NAT?NAPT 有哪些特点？NAT 的优点和缺点有哪些？NAT 的优点和缺点有哪些？

答案：P173-174

第 5 章　传输层

5—01　试说明运输层在协议栈中的地位和作用，运输层的通信和网络层的通信有什么重要区别？为什么运输层是必不可少的？

答：运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，必须由运输层以复用和分用的形式加载到网络层。

5—02　网络层提供数据报或虚电路服务对上面的运输层有何影响？

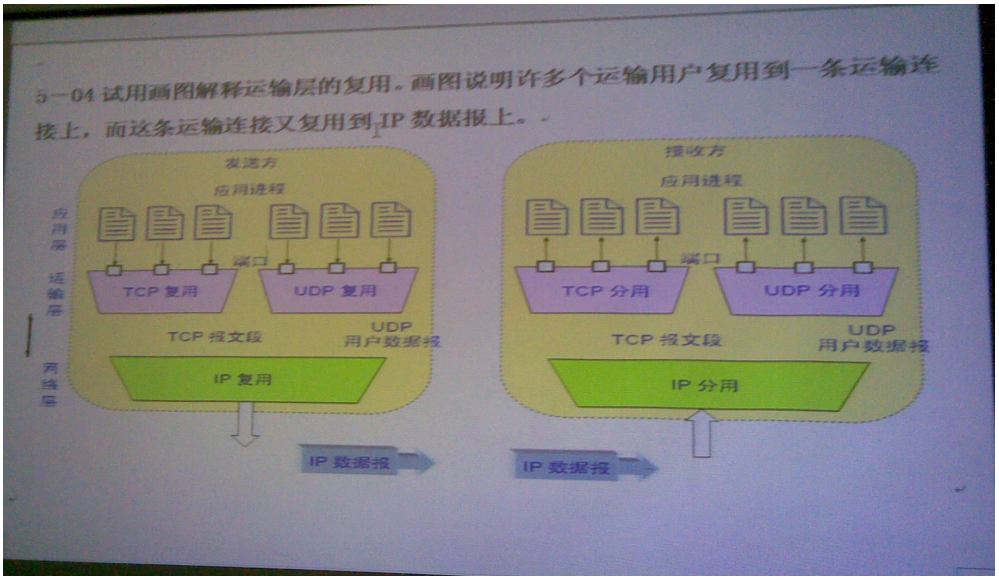
答：网络层提供数据报或虚电路服务不影响上面的运输层的运行机制。

但提供不同的服务质量。

5—03　当应用程序使用面向连接的 TCP 和无连接的 IP 时，这种传输是面向连接的还是面向无连接的？

答：都是。这要在不同层次来看，在运输层是面向连接的，在网络层则是无连接的。

5—04　试用画图解释运输层的复用。画图说明许多个运输用户复用到一条运输连接上，而这条运输连接有复用到 IP 数据报上。



5—05　试举例说明有些应用程序愿意采用不可靠的 UDP，而不用采用可靠的 TCP。

答：VOIP：由于语音信息具有一定的冗余度，人耳对 VOIP 数据报损失由一定的承受度，但对传输时延的变化较敏感。

有差错的 UDP 数据报在接收端被直接抛弃，TCP 数据报出错则会引起重传，可能带来较大的时延扰动。

因此 VOIP 宁可采用不可靠的 UDP，而不愿意采用可靠的 TCP。

5—06　接收方收到有差错的 UDP 用户数据报时应如何处理？

答：丢弃

5—07 如果应用程序愿意使用 UDP 来完成可靠的传输，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。

5—08 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（无边界约束，课分拆/合并），但维持各字节

5—09 端口的作用是什么？为什么端口要划分为三种？

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。

熟知端口，数值一般为 0~1023.标记常规的服务进程；

登记端口号，数值为 1024~49151，标记没有熟知端口号的非常规的服务进程；

5—10 试说明运输层中伪首部的作用。

答：用于计算运输层数据报校验和。

5—11 某个应用进程使用运输层的用户数据报 UDP，然而继续向下交给 IP 层后，又封装成 IP 数据报。既然都是数据报，可否跳过 UDP 而直接交给 IP 层？哪些功能 UDP 提供了但 IP 没提提供？

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。

5—12 一个应用程序用 UDP，到 IP 层把数据报在划分为 4 个数据报片发送出去，结果前两个数据报片丢失，后两个到达目的站。过了一段时间应用程序重传 UDP，而 IP 层仍然划分为 4 个数据报片来传送。结果这次前两个到达目的站而后两个丢失。试问：在目的站能否将这两次传输的 4 个数据报片组装成完整的数据报？假定目的站第一次收到的后两个数据报片仍然保存在目的站的缓存中。

答：不行

重传时，IP 数据报的标识字段会有另一个标识符。

仅当标识符相同的 IP 数据报片才能组装成一个 IP 数据报。

前两个 IP 数据报片的标识符与后两个 IP 数据报片的标识符不同，因此不能组装成一个 IP 数据报。

5—13 一个 UDP 用户数据的数据字段为 8192 季节。在数据链路层要使用以太网来传送。试问应当划分为几个 IP 数据报片？说明每一个 IP 数据报字段长度和片偏移字段的值。

答：6 个

数据字段的长度：前 5 个是 1480 字节，最后一个是 800 字节。

片偏移字段的值分别是：0，1480，2960，4440，5920 和 7400.

5—14　一 UDP 用户数据报的首部十六进制表示是：06 32 00 45 00 1C　E2 17.试求源端口、目的端口、用户数据报的总长度、数据部分长度。这个用户数据报是从客户发送给服务器发送给客户？使用 UDP 的这个服务器程序是什么？

解：源端口 1586，目的端口 69，UDP 用户数据报总长度 28 字节，数据部分长度 20 字节。

此 UDP 用户数据报是从客户发给服务器（因为目的端口号<1023，是熟知端口）、服务器程序是 TFFTP。

5—15　使用 TCP 对实时话音数据的传输有没有什么问题？使用 UDP 在传送数据文件时会有什么问题？

答：如果语音数据不是实时播放（边接受边播放）就可以使用 TCP，因为 TCP 传输可靠。接收端用 TCP 讲话音数据接受完毕后，可以在以后的任何时间进行播放。但假定是实时传输，则必须使用 UDP。

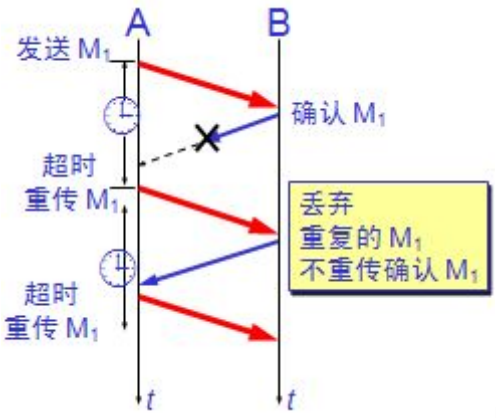
UDP 不保证可靠交付，但 UCP 比 TCP 的开销要小很多。因此只要应用程序接受这样的服务质量就可以使用 UDP。

5—16　在停止等待协议中如果不使用编号是否可行？为什么？

答:分组和确认分组都必须进行编号，才能明确哪个分则得到了确认。

5—17　在停止等待协议中，如果收到重复的报文段时不予理睬（即悄悄地丢弃它而其他什么也没做）是否可行？试举出具体的例子说明理由。

答：

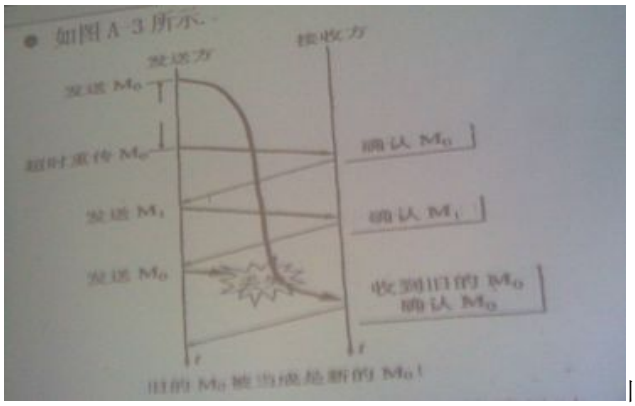


收到重复帧不确认相当于确认丢失

5—18　假定在运输层使用停止等待协议。发送发在发送报文段 M0 后再设定的时间内未收到确认，于是重传 M0，但 M0 又迟迟不能到达接收方。不久，发送方收到了迟到的对 M0 的确认，于是发送下一个报文段 M1，不久就收到了对 M1 的确认。接着发送方发送新的报文段 M0，但这个新的 M0 在传送过程中丢失了。正巧，一开始就滞留在网络中的 M0 现在到达接收方。接收方无法分辨 M0 是旧的。于是收下 M0，并发送确认。显然，接收方后来收到的 M0 是重复的，协议失败了。

试画出类似于图 5-9 所示的双方交换报文段的过程。

答：



旧的 M0 被当成新的 M0。

5—19　试证明：当用 n 比特进行分组的编号时，若接收到窗口等于 1（即只能按序接收分组），当仅在发送窗口不超过 2^n-1 时，连接 ARQ 协议才能正确运行。窗口单位是分组。

解：见课后答案。

5—20　在连续 ARQ 协议中，若发送窗口等于 7，则发送端在开始时可连续发送 7 个分组。因此，在每一分组发送后，都要置一个超时计时器。现在计算机里只有一个硬时钟。设这 7 个分组发出的时间分别为 t0,t1…t6,且 tout 都一样大。试问如何实现这 7 个超时计时器（这叫软件时钟法）？

解：见课后答案。

5—21　假定使用连续 ARQ 协议中，发送窗口大小事 3，而序列范围[0,15],而传输媒体保证在接收方能够按序收到分组。在某时刻，接收方，下一个期望收到序号是 5.

试问：

（1）　在发送方的发送窗口中可能有出现的序号组合有哪几种？

（2）　接收方已经发送出去的、但在网络中（即还未到达发送方）的确认分组可能有哪些？说明这些确认分组是用来确认哪些序号的分组。

5—22　主机 A 向主机 B 发送一个很长的文件，其长度为 L 字节。假定 TCP 使用的 MSS 有 1460 字节。

（1）　在 TCP 的序号不重复使用的条件下，L 的最大值是多少？

（2）　假定使用上面计算出文件长度，而运输层、网络层和数据链路层所使用的首部开销共 66 字节，链路的数据率为 10Mb/s，试求这个文件所需的最短发送时间。

解：（1）L_max 的最大值是 2^32=4GB,G=2^30.

(2) 满载分片数 Q={L_max/MSS}取整=2941758 发送的总报文数

N=Q*(MSS+66)+{（L_max-Q*MSS）+66}=4489122708+682=4489123390

总字节数是 N=4489123390 字节，发送 4489123390 字节需时间为：N*8/（10*10^6）=3591.3 秒，即 59.85 分，约 1 小时。

5—23　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 A 发送的第二个报文段中的数据有多少字节？

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

解：（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

5—24 一个 TCP 连接下面使用 256kb/s 的链路，其端到端时延为 128ms。经测试，发现吞吐量只有 120kb/s。试问发送窗口 W 是多少？（提示：可以有两种答案，取决于接收等发出确认的时机）。

解：

来回路程的时延等于 256ms(=128ms×2).设窗口值为 X(注意:以字节为单位),假定一次最大发送量等于窗口值,且发射时间等于 256ms,那么,每发送一次都得停下来期待再次得到下一窗口的确认,以得到新的发送许可.这样,发射时间等于停止等待应答的时间,结果,测到的平均吞吐率就等于发送速率的一半,即

8X÷(256×1000)=256×0.001

X=8192

所以,窗口值为 8192.

5—25 为什么在 TCP 首部中要把 TCP 端口号放入最开始的 4 个字节？

答：在 ICMP 的差错报文中要包含 IP 首部后面的 8 个字节的内容，而这里面有 TCP 首部中的源端口和目的端口。当 TCP 收到 ICMP 差错报文时需要用这两个端口来确定是哪条连接出了差错。

5—26 为什么在 TCP 首部中有一个首部长度字段，而 UDP 的首部中就没有这个这个字段？

答：TCP 首部除固定长度部分外，还有选项，因此 TCP 首部长度是可变的。UDP 首部长度是固定的。

5—27 一个 TCP 报文段的数据部分最多为多少个字节？为什么？如果用户要传送的数据的字节长度超过 TCP 报文字段中的序号字段可能编出的最大序号，问还能否用 TCP 来传送？

答：65495 字节，此数据部分加上 TCP 首部的 20 字节，再加上 IP 首部的 20 字节，正好是 IP 数据报的最大长度 65535.（当然，若 IP 首部包含了选择，则 IP 首部长度超过　　20 字节，这时 TCP 报文段的数据部分的长度将小于 65495 字节。）
数据的字节长度超过 TCP 报文段中的序号字段可能编出的最大序号，通过循环使用序号，仍能用 TCP 来传送。

5—28　主机 A 向主机 B 发送 TCP 报文段，首部中的源端口是 m 而目的端口是 n。当 B 向 A 发送回信时，其 TCP 报文段的首部中源端口和目的端口分别是什么？

答：分别是 n 和 m。

5—29　在使用 TCP 传送数据时，如果有一个确认报文段丢失了，也不一定会引起与该确认报文段对应的数据的重传。试说明理由。

答：还未重传就收到了对更高序号的确认。

5—30　设 TCP 使用的最大窗口为 65535 字节，而传输信道不产生差错，带宽也不受限制。若报文段的平均往返时延为 20ms，问所能得到的最大吞吐量是多少?

答:在发送时延可忽略的情况下,最大数据率=最大窗口*8/平均往返时间=26.2Mb/s。

5—31　通信信道带宽为 1Gb／s，端到端时延为 10ms。TCP 的发送窗口为 65535 字节。试问:可能达到的最大吞吐量是多少?信道的利用率是多少?

答：
L=65536×8+40×8=524600
C=109b/s
L/C=0.0005246s
Td=10×10-3s
0.02104864
Throughput=L/(L/C+2×Td)=524600/0.0205246=25.5Mb/s
Efficiency=(L/C)//(L/C+2×D)=0.0255
最大吞吐量为 25.5Mb/s。信道利用率为 25.5/1000=2.55%

5—32　什么是 Karn 算法?在 TCP 的重传机制中，若不采用 Karn 算法，而是在收到确认时都认为是对重传报文段的确认，那么由此得出的往返时延样本和重传时间都会偏小。试问：重传时间最后会减小到什么程度?

答：Karn 算法：在计算平均往返时延 RTT 时，只要报文段重传了，就不采用其往返时延样本。
设新往返时延样本 Ti
RTT（1）=a*RTT（i-1）+（1-a）*T（i）；
RTT^（i）=a* RTT（i-1）+（1-a）*T（i）/2；
RTT（1）=a*0+(1-a)*T(1)= (1-a)*T(1);
RTT^（1）=a*0+(1-a)*T(1)/2= RTT（1）/2
RTT（2）= a*RTT（1）+（1-a）*T（2);
RTT^（2）= a*RTT（1）+（1-a）*T（2)/2;
　　= a*RTT（1）/2+（1-a）*T（2)/2= RTT（2）/2
RTO=beta*RTT,在统计意义上，重传时间最后会减小到使用 karn 算法的 1/2.

5—33　假定 TCP 在开始建立连接时，发送方设定超时重传时间是 RTO=6s。

（1）当发送方接到对方的连接确认报文段时，测量出 RTT 样本值为 1.5s。试计算现在的 RTO 值。

（2）当发送方发送数据报文段并接收到确认时，测量出 RTT 样本值为 2.5s。试计算现在的 RTO 值。

答：

（1）据 RFC2988 建议，RTO=RTTs+4*RTTd。其中 RTTd 是 RTTs 的偏差加权均值。

初次测量时，RTTd（1）= RTT（1）/2；

后续测量中，RTTd（i）=（1-Beta）* RTTd（i-1）+Beta*{ RTTs- RTT（i）}；

Beta=1/4

依题意，RTT（1）样本值为 1.5 秒，则

RTTs（1）=RTT（1）=1.5s　　RTTd(1)=RTT(1)/2=0.75s

RTO(1)=RTTs(1)+4RTTd(1)=1.5+4*0.75=4.5(s)

（2）RTT（2）=2.5　　RTTs（1）=1.5s　　RTTd（1）=0.75s

RTTd（2）=（1-Beta）* RTTd（1）+Beta*{ RTTs（1）- RT

（2）}=0.75*3/4+{1.5-2.5}/4=13/16

RTO(2)=RTTs（1）+4RTTd（2）=1.5+4*13/16=4.75s

5—34　已知第一次测得 TCP 的往返时延的当前值是 30 ms。现在收到了三个接连的确认报文段，它们比相应的数据报文段的发送时间分别滞后的时间是：26ms，32ms 和 24ms。设α=0．9。试计算每一次的新的加权平均往返时间值 RTTs。讨论所得出的结果。

答：a=0.1，　RTTO=30

RTT1=RTTO*(1-a) +26*a=29.6

RTT2=RTT1*a+32(1-a)=29.84

RTT3=RTT2*a+24（1-a）=29.256

三次算出加权平均往返时间分别为 29.6，29.84 和 29.256ms。

可以看出，RTT 的样本值变化多达 20%时，加权平均往返

5—35　试计算一个包括 5 段链路的运输连接的单程端到端时延。5 段链路程中有 2 段是卫星链路，有 3 段是广域网链路。每条卫星链路又由上行链路和下行链路两部分组成。可以取这两部分的传播时延之和为 250ms。每一个广域网的范围为 1500km，其传播时延可按 150000km／s 来计算。各数据链路速率为 48kb／s，帧长为 960 位。

答：5 段链路的传播时延=250*2+（1500/150000）*3*1000=530ms

5 段链路的发送时延=960/（48*1000）*5*1000=100ms

所以 5 段链路单程端到端时延=530+100=630ms

5—36　重复 5-35 题，但假定其中的一个陆地上的广域网的传输时延为 150ms。

答：760ms

5—37　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?这里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。

快重传算法规定：

发送端只要一连收到三个重复的 ACK 即可断定有分组丢失了，就应该立即重传丢手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：

当发送端收到连续三个重复的 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，以大大减少注入到网络中的分组数。

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。

5—38 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.

5—39 TCP 的拥塞窗口 cwnd 大小与传输轮次 n 的关系如下所示：

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

（1）试画出如图 5-25 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三个重复的确认还是通过超市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 轮次之后收到了三个重复的确认，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）拥塞窗口与传输轮次的关系曲线如图所示（课本后答案）：

（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三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.

5—40 TCP 在进行流量控制时是以分组的丢失作为产生拥塞的标志。有没有不是因拥塞而引起的分组丢失的情况?如有，请举出三种情况。

答：

当 Ip 数据报在传输过程中需要分片，但其中的一个数据报未能及时到达终点，而终点组装 IP 数据报已超时，因而只能丢失该数据报；IP 数据报已经到达终点，但终点的缓存没有足够的空间存放此数据报；数据报在转发过程中经过一个局域网的网桥，但网桥在转发该数据报的帧没有足够的差错空间而只好丢弃。

5—41 用 TCP 传送 512 字节的数据。设窗口为 100 字节，而 TCP 报文段每次也是传送 100 字节的数据。再设发送端和接收端的起始序号分别选为 100 和 200，试画出类似于图 5-31 的工作示意图。从连接建立阶段到连接释放都要画上。

5—42 在图 5-32 中所示的连接释放过程中，主机 B 能否先不发送 ACK=x+1 的确认？ (因为后面要发送的连接释放报文段中仍有 ACK=x+1 这一信息)

答：

如果 B 不再发送数据了，是可以把两个报文段合并成为一个，即只发送 FIN+ACK 报文段。但如果 B 还有数据报要发送，而且要发送一段时间，那就不行，因为 A 迟迟收不到确认，就会以为刚才发送的 FIN 报文段丢失了，就超时重传这个 FIN 报文段，浪费网络资源。

5—43 在图(5-33)中，在什么情况下会发生从状态 LISTEN 到状态 SYN_SENT，以及从状态 SYN_ENT 到状态 SYN_RCVD 的变迁?

答：当 A 和 B 都作为客户，即同时主动打开 TCP 连接。这时的每一方的状态变迁都是：CLOSED----→SYN-SENT---→SYN-RCVD--→ESTABLISHED

5—44 试以具体例子说明为什么一个运输连接可以有多种方式释放。可以设两个互相通信的用户分别连接在网络的两结点上。

答：设 A,B 建立了运输连接。协议应考虑一下实际可能性：

A 或 B 故障，应设计超时机制，使对方退出，不至于死锁；

A 主动退出，B 被动退出

B 主动退出，A 被动退出

5—45 解释为什么突然释放运输连接就可能会丢失用户数据，而使用 TCP 的连接释放方法就可保证不丢失数据。

答：

当主机 1 和主机 2 之间连接建立后，主机 1 发送了一个 TCP 数据段并正确抵达主机 2，接着主机 1 发送另一个 TCP 数据段，这次很不幸，主机 2 在收到第二个 TCP 数据段之前发出了释放连接请求，如果就这样突然释放连接，显然主机 1 发送的第二个 TCP 报文段会丢失。

而使用 TCP 的连接释放方法，主机 2 发出了释放连接的请求，那么即使收到主机 1 的确认后，只会释放主机 2 到主机 1 方向的连接，即主机 2 不再向主机 1 发送数据，而仍然可接受主机 1 发来的数据，所以可保证不丢失数据。

5—46 试用具体例子说明为什么在运输连接建立时要使用三次握手。说明如不这样做可能会出现什么情况。

答：

3 次握手完成两个重要的功能，既要双方做好发送数据的准备工作（双方都知道彼此已准备好），也要允许双方就初始序列号进行协商，这个序列号在握手过程中被发送和确认。

假定 B 给 A 发送一个连接请求分组，A 收到了这个分组，并发送了确认应答分组。按照两次握手的协定，A 认为连接已经成功地建立了，可以开始发送数据分组。可是，B 在 A 的应答分组在传输中被丢失的情况下，将不知道 A 是否已准备好，不知道 A 建议什么样的序列号，B 甚至怀疑 A 是否收到自己的连接请求分组，在这种情况下，B 认为连接还未建立成功，将忽略 A 发来的任何数据分组，只等待连接确认应答分组。

而 A 发出的分组超时后，重复发送同样的分组。这样就形成了死锁。

5—47 一个客户向服务器请求建立 TCP 连接。客户在 TCP 连接建立的三次握手中的最后一个报文段中捎带上一些数据，请求服务器发送一个长度为 L 字节的文件。假定：

（1）客户和服务器之间的数据传输速率是 R 字节/秒，客户与服务器之间的往返时间是 RTT（固定值）。

（2）服务器发送的 TCP 报文段的长度都是 M 字节，而发送窗口大小是 nM 字节。

（3）所有传送的报文段都不会出错（无重传），客户收到服务器发来的报文段后就及时发送确认。

（4）所有的协议首部开销都可忽略，所有确认报文段和连接建立阶段的报文段的长度都可忽略（即忽略这些报文段的发送时间）。

试证明，从客户开始发起连接建立到接收服务器发送的整个文件多需的时间 T 是：

T=2RTT+L/R 当 nM>R(RTT)+M

或 T=2RTT+L/R+(K-1)[M/R+RTT-nM/R] 当 nM<R(RTT)+M

其中，K=[L/nM]，符号[x]表示若 x 不是整数，则把 x 的整数部分加 1。

解：

发送窗口较小的情况，发送一组 nM 个字节后必须停顿下来，等收到确认后继续发送。

共需 K=[L/nM]个周期：其中

前 K-1 个周期每周期耗时 M/R+RTT,共耗时（K-1）（M/R+RTT）

第 K 周期剩余字节数 Q=L-（K-1）*nM，需耗时 Q/R

总耗时=2*RTT+(K-1)M/(R+RTT)+Q/R=2*RTT+L/R+(K-1)[(M/R+RTT)-nM/R

第 6 章　应用层

6-01　因特网的域名结构是怎么样的？它与目前的电话网的号码结构有何异同之处？

答：

（1）域名的结构由标号序列组成，各标号之间用点隔开：

…．三级域名．二级域名．顶级域名

各标号分别代表不同级别的域名。

（2）电话号码分为国家号结构分为（中国 +86）、区号、本机号。

6-02　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权服务器有何区别？

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。

因特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。因特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。

6-03　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。

6-04　设想有一天整个因特网的 DNS 系统都瘫痪了（这种情况不大会出现），试问还可以给朋友发送电子邮件吗？

答：不能；

6-05　文件传送协议 FTP 的主要工作过程是怎样的？为什么说 FTP 是带外传送控制信息？主进程和从属进程各起什么作用？

答：

（1）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。

主进程的工作步骤：

1、打开熟知端口（端口号为 21），使客户进程能够连接上。

2、等待客户进程发出连接请求。

3、启动从属进程来处理客户进程发来的请求。从属进程对客户进程的请求处理完毕后即终止，但从属进程在运行期间根据需要还可能创建其他一些子进程。

4、回到等待状态，继续接受其他客户进程发来的请求。主进程与从属进程的处理是并发地进行。

FTP 使用两个 TCP 连接。

控制连接在整个会话期间一直保持打开，FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。

实际用于传输文件的是“数据连接”。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”，用来连接客户端和服务器端的数据传送进程。

数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

6-06 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：

（1）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。

6-07 远程登录 TELNET 的主要特点是什么？什么叫做虚拟终端 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。

6-08 解释以下名词。各英文缩写词的原文是什么？

www,URL.HTTP,HTML,CGI,浏览器，超文本，超媒体，超链，页面，活动文档，

搜索引擎。

答：

www:万维网 WWW（World Wide Web）并非某种特殊的计算机网络。万维网是一个大规模的、联机式的信息储藏所，英文简称为 Web.万维网用链接的方法能非常方便地从因特网上的一个站点访问另一个站点（也就是所谓的“链接到另一个站点”），从而主动地按需获取丰富的信息。

URL:为了使用户清楚地知道能够很方便地找到所需的信息，万维网使用统一资源定位符 URL（Uniform Resource Locator）来标志万维网上的各种文档，并使每一个文档在整个因特网的范围内具有唯一的标识符 URL.

HTTP:为了实现万维网上各种链接，就要使万维网客户程序与万维网服务器程序之间的交互遵守严格的协议，这就是超文本传送协议 HTTP.HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。

CGI:通用网关接口 CGI 是一种标准，它定义了动态文档应该如何创建，输入数据应如何提供给应用程序，以及输出结果意如何使用。CGI 程序的正式名字是 CGI 脚本。按照计算机科学的一般概念。

浏览器：一个浏览器包括一组客户程序、一组解释程序，以及一个控制程序。

超文本：超文本的基本特征就是可以超链接文档；你可以指向其他位置，该位置可以在当前的文档中、局域网中的其他文档，也可以在因特网上的任何位置的文档中。这些文档组成了一个杂乱的信息网。目标文档通常与其来源有某些关联，并且丰富了来源；来源中的链接元素则将这种关系传递给浏览者。

超媒体：超级媒体的简称,是超文本（hypertext）和多媒体在信息浏览环境下的结合。

超链：超链接可以用于各种效果。超链接可以用在目录和主题列表中。浏览者可以在浏览器屏幕上单击鼠标或在键盘上按下按键，从而选择并自动跳转到文档中自己感兴趣的那个主题，或跳转到世界上某处完全不同的集合中的某个文档。超链接（hyper text），或者按照标准叫法称为锚（anchor），是使用 <a> 标签标记的，可以用两种方式表示。锚的一种类型是在文档中创建一个热点，当用户激活或选中（通常是使用鼠标）这个热点时，会导致浏览器进行链接。

页面：页面，类似于单篇文章页面，但是和单篇文章不同的是：1.每个页面都可以自定义样式，而单篇文章则共用一个样式。2.页面默认情况一般不允许评论，而单篇文章默认情况允许评论。3.页面会出现在水平导航栏上，不会出现在分类和存档里，而单篇文章会出现在分类和存档里，不会出现在水平导航栏上。

活动文档：即正在处理的文档。在 Microsoft Word 中键入的文本或插入的图形将出现在活动文档中。活动文档的标题栏是突出显示的。一个基于 Windows 的、嵌入到浏览器中的非 HTML 应用程序，提供了从浏览器界面访问这些应用程序的　　功能的方法。

搜索引擎：搜索引擎指能够自动从互联网上搜集信息，经过整理以后，提供给用户进行查阅的系统。

6-09 假定一个超链从一个万维网文档链接到另一个万维网文档时，由于万维网文档上出现了差错而使得超链只想一个无效的计算机名字。这是浏览器将向用户报告什么？

答：404 Not Found。

6-10 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）。

6-11 你所使用的浏览器的高速缓存有多大？请进行一个试验：访问几个万维网文档，然后将你的计算机与网络断开，然后再回到你刚才访问过的文档。你的浏览器的高速缓存能够存放多少各页面？

答：（因不同机器而定）

6-12 、什么是动态文档？试举出万维网使用动态文档的一些例子。

答案：如果文挡的内容在浏览器访问万维网时才有应用程序动态创建，这种文档称为动态文档（dynamic document）。当浏览器请求到达时，万维网服务器要运行另一个应用程序，并将控制转移到此程序。接着，该应用程序对浏览器发来的数据进行处理，其间可能访问数据库或图形软件包等其它服务器资源，并输出 HTML 格式的文档，万维网服务器将应用程序的输出作为对浏览器的响应。由于对浏览器每次请求的响应都是临时生成的，因此用户通过动态文档看到的内容可根据需要不断变化。例如 Google 搜索到的信息，博客，论坛等。

6-13、浏览器同时打开多个 TCP 连接进行浏览的优缺点如何？请说明理由。

答案：优点：简单明了方便。

缺点：卡的时候容易死机

6-14、当使用鼠标点取一个 WWW 文档时，若该文档除了有文本外，还有一个本地.gif 图像和两个远地.gif 图像。试问：需要使用哪个应用程序，以及需要建立几次 UDP 连接和几次 TCP 连接？

解答

使用支持 HTTP 协议的应用程序。不需要建立 UDP 连接。需要建立 4 次 TCP 连接，一次读取整个 WWW 文档，然后读取三个.gif 图像文件。由于 HTTP 是一种分布式协议，对本地.gif 图像文件和远地.gif 图像文件同样看待。

6-15、假定你在浏览器上点击一个 URL,但是这个 URL 的 IP 地址以前并没有缓存在本地主机上。因此需要用 DNS 自动查找和解析。假定要解析到所有要找到的 URLd IP 地址公斤过 n 个 DNS 服务器，所经过的时间分别为 RTT1,RTT2,…,RTTn。假定从要找的网页上只需读取一个很小的图片(即忽略这个小图片的传输时间)。从本地主机到这个网页的往返时间是 RTTw。试问从点击这个 URL 开始，一直到本地主机的屏幕上出现所读取的小图片，一共要经过多少时间？

解：解析 IP 地址需要时间是：RTT1+RTT2+…+RTTn。

建立 TCP 连接和请求万维网文档需要 2RTTw。

6-16、在上题中假定同一台服务器的 HTML 文件中有链接了三个份非常小的对象。若忽略这些对象的发送时间，试计算客户点击读取这些对象所需的时间。

(1) 没有并行 TCP 连接的非持续 HTTP；

(2) 使用并行 TCP 连接的非持续 HTTP；

(3) 流水线方式的持续 HTTP。

解：（1）所需时间=RTT1+RTT2+…+RTTn+8RTTw。

（2）所需时间=RTT1+RTT2+…+RTTn+4RTTw。

（3）所需时间=RTT1+RTT2+…+RTTn+3RTTw。

6-17、在浏览器中应当有几个可选解释程序。试给出一些可选解释程序的名称。

答：在浏览器中，HTML 解释程序是必不可少的，而其他的解释程序则是可选的。如 java 可选解释程序，但是在运行 java 的浏览器是则需要两个解释程序，即 HTML 解释程序和 Java 小应用程序解释程序。

6-18、一个万维网网点有 1 千万个页面，平均每个页面有 10 个超链。读取一个页面平均要 100ms。问要检索整个网点所需的最少时间？

答：$t=100*10^{-3}*10*1000*10^{4}=10^{7}$ s

6-19、搜索引擎可分为那两种类型？给有什么特点？

答案：

搜索引擎按其工作方式主要可分为两种，分别是全文搜索引擎（Full Text Search Engine）和目录索引类搜索引擎（Search Index/Directory

全文搜索引擎

全文搜索引擎是名副其实的搜索引擎，国外具代表性的有 Google、Fast/AllTheWeb、AltaVista、Inktomi、Teoma、WiseNut 等，国内著名的有百度（Baidu）。它们都是通过从互联网上提取的各个网站的信息（以网页文字为主）而建立的数据库中，检索与用户查询条件匹配的相关记录，然后按一定的排列顺序将结果返回给用户，因此他们是真正的搜索引擎。从搜索结果来源的角度，全文搜索引擎又可细分为两种，一种是拥有自己的检索程序（Indexer），俗称“蜘蛛”（Spider）程序或“机器人”（Robot）程序，并自建网页数据库，搜索结果直接从自身的数据库中调用，如上面提到的 7 家引擎；另一种则是租用其他引擎的数据库，并按自定的格式排列搜索结果，如 Lycos 引擎。

目录索引

目录索引虽然有搜索功能，但在严格意义上算不上是真正的搜索引擎，仅仅是按目录分类的网站链接列表而已。用户完全可以不用进行关键词（Keywords）查询，仅靠分类目录也可找到需要的信息。目录索引中最具代表性的莫过于大名鼎鼎的 Yahoo 雅虎。其他著名的还有 Open Directory Project（DMOZ）、LookSmart、About 等。国内的搜狐、新浪、网易搜索也都属于这一类

6-20 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？

答案：电子邮件的主要组成部件，这就是用户代理、邮件服务器，以及电子邮件使用的协议。用户代理 UA 就是用户与电子邮件系统的接口，在大多数情况下就是在用户 PC 机中运行的程序。邮件服务器是电子邮件系统的核心构建，因特网上所有的 ISP 都有邮件服务器。遇见服务器所使用的协议主要有用户发送邮件的 SMTP 协议，另一个协议是用于接受邮件的 POP 协议。

用户代理的功能主要有：（1）撰写，给用户提供方便地编辑信件的环境；（2）显示，能方便的在计算机屏幕上显示出来信；（3）处理，处理包括发送邮件和接收邮件。

没有用户代理是不行的。这是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，每天不间断地连接在因特网上，否则可能使很陡外面发来的邮件丢失。让用户的 PC 机运行邮件服务器程序是不现实的。让来信暂时存储在 ISP 邮件服务器中，而当用户方便是就从服务器中

的用户信箱中来读取来信，是比较合理的做法。

6-21 电子邮件的信封和内容在邮件的传送过程中起什么作用？和用户的关系如何？

答案 电子邮件由信封和内容两部分组成。电子邮件的传输程序根据邮件信封上的信息来传送邮件，用户在从自己的邮箱中读取邮件时候才能见到邮件的内容。

6-22 电子邮件的地址格式是怎样的？请说明各部分的意思。

答案 电子邮件系统规定电子邮件地址的格式为：收信人邮箱名@邮箱所在主机的域名，其中“@”表示“在”的意思。收信人邮箱名又简称为用户名，是收信人自己定义的字符串标识符，收信人邮箱名的字符串在邮箱所在计算机中必须是唯一的，电子邮件的用户一般采用容易记忆的字符串。邮箱所在地域名在整个因特网范围内必须是唯一的。

6-23 试简述 SMTP 通信的三个阶段的过程。

答案 SMTP 通信的三个阶段：

1.连接建立。发信人现将发送的邮件送到邮件缓存。SMTP 客户每隔一段时间对邮件缓存扫描一次。如发现有邮件，就通主机的 SMTP 服务器建立 TCP 连接，连接建立后，SMTP 服务器发出“服务就绪”，然后 SMTP 客户想 SMTP 发送命令，SMTP 若有能力接收邮件，发送准备好命令，若 SMTP 服务器不可用，回答服务不可用。

2.邮件传送。邮件的发送从 MAIL 命令开始。若 SMTP 服务器已经准备号接受邮件，则发送一个 RCPT 命令，并从 SMTP 服务器返回相应的信息，然后开始传送数据；如果 SMTP 没有准备好接受邮件，就返回一个代码，指出错误的原因。

3.连接释放。邮件发送完毕后，SMTP 客户发送 QUIT 命令。SMTP 服务器返回信息，表示同意释放 TCP 连接，邮件发送的全部过程结束。

6-24 试述邮局协议 POP 的工作过程。在电子邮件中，为什么需要使用 POP 和 SMTP 这两个协议？IMAP 与 POP 有何区别？

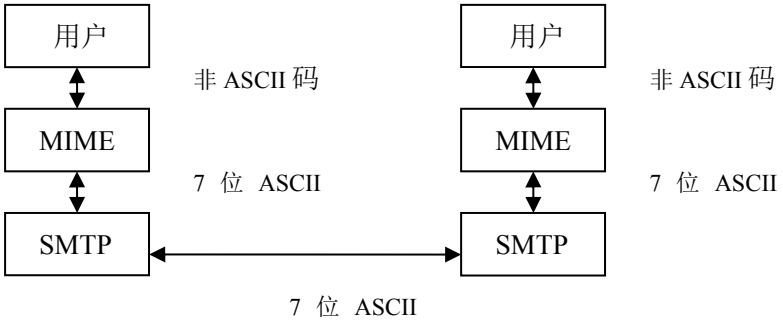
答案 当收取邮件时，电子邮件软件首先会根据用户名和密码调用 DNS 协议对 POP 服务器进行解析 I P 地址，然后邮件程序便开始使用 TCP 协议连接邮件服务器的 110 端口。当邮件程序成功地连上 POP 服务器后，齐贤慧使用 USER 命令将邮箱的账号传给 pop 服务器，然后在使用 PASS 命令将邮箱的密码传给服务器，当完成这一认证过程后，邮件程序使用 STAT 命令请求服务器返回邮箱的统计资料，比如邮件总数和邮件大小等，然后 LIST 便会列出服务器里邮件数量。接着邮件程序就会使用 RETR 命令接受邮件，接受一封后便使用 DELE 命令将邮件服务器中的邮件置为删除状态。当使用 QUIT 时，邮件服务器便会将置为删除标志的邮件给删了。这就是 POP 协议工作的过程。

pop 协议和 SMTP 协议分别是用来收信、发信时使用的协议。也就是说，这两个协议是专门为接受、发送邮件设计的语言，通过使用 pop 和 SMTP 协议，可以是接受以及发送邮件变得方便。

因特网报文存取协议 IMAP 比 pop 复杂，虽然都是按照客户服务器方式工作，但还是有很大的差别。IMAP 是一个联机协议，用户可以在自己的 PC 机上操纵 ISP 邮件服务器的邮箱，就像在本地操纵一样。当用户打开 IMAP 服务器的邮箱时，可以看到邮件首部。若用户需要打开某个邮件，则该邮件才传送到用户的计算机上。用户可以按照某种条件对邮件进行查找，在用户未发出删除邮件的命令之前，IMAP 服务器邮箱中的邮件一直保存着。这样用户就可以在不同的地方使用不同的计算机随时上网阅读和处理自己的邮件。IMAP 还允许收信人只读取邮件中的某一个部分。

6-25 MIME 与 SMTP 的关系是怎样的？什么是 quoted-printable 编码和 base64 编码?

答案 由于 SMTP 存在着一些缺点和不足，在这种情况下提出了通用因特网邮件扩充协议 MIME。MIME 并没有改动 SMTP 或取代它。MIME 的意图是继续使用目前的格式，但增加了邮件主题的结构，并定义了传送非 ASCII 码的编码规则，也就是说，MIME 邮件可以在现有的电子邮件程序和协议下传送。可以用题 8-12 解图表示。



题 8-12 解图

quoted-printable 编码适用于所有可以打印的 ASCII 码，除非特殊字符等号“=”外，都不改变。

base64 编码适用于任意的二进制文件。编码过程是先将二进制代码划分为一个 24bit 长的单元，然后将每一个 24bit 单元划分为 4 个 6bit 组，每一个 6bit 组按照一定方法转换成
ASCII 码。base64 编码增加了开销，当需要传送的数据大部分为 ASCII 码时，最好还是采用 quoted-printable 编码。

6-26 一个二进制文件共 3072 字节长，若使用 base64 编码，并且每发送完 80 字节就插入一个回车符 CR 和一个换行符 LF，问一共发送了多少个字节？

解析 base64 的编码原则方法是先将二进制代码划分为一个 24bit 长的单元，然后将每
一个 24bit 单元划分为 4 个 6bit 组，每一个 6bit 组按照一下方法转换成 ASCII 码。6bit 的二进制代码共有 64 中不同的值，从 0 到 63，分别用大写字码，小写字码，10 个阿拉伯数字,+,/表示,再用两个连在一起的等号和一个等号分别表示最后一组的代码只有 8 或 16bit。回车和换行可以在任何地方插入。然后将 ASCII 码进行传输。简单说，是将每 6bit 的数据转换为 8bit 之后再进行传输。

答案 转换后共需要传送的字节数=3072*8/4096,由题知每 80 个字节就插入两个字节，所以一共还需要插入的字节数为 4096/80*2=102 再加上最后一组发送完应歙如的 CR 和 LF，最后一共需要传输的字节数为 4096+102+2=4100（字节）。

6-27 试将数据 11001100 10000001 00111000 进行 base64 编码，并得出最后传送的 ASCII 数据。

解析 考察的仍然是 base64 编码，基本原理同上体一样。分成 6bit 每组，按照相对应
的 ASCII 码进行传送。本题中按照 6bit 每组进行排列，得到 110011 001000 000100 111000，

相对应的编码为 z1E4,如题 8-14 解图所示为 ASCII 码表。

根据 ASCII 编码表得到最后传送的数据为：7A 49 45 34。

答案 01111010 01001001 01000101 00110100。

6-28 试将数据 01001100 10011101 00111001 进行 quoted-printable 编码，并得出最后传送
的 ASCII 数据。这样的数据用 quoted-printable 编码后，其编码开销有多大？

解析 quoted-printable 编码规则是对于可打印的字节的二进制代码用两个十六进制
数字表示，然后在前面加上一个等号“=”。而等号的二进制代码为 00111101，即十六进制的 3D，等号的 quoted-printable 编码为“=3D”。对于本体，所给数据的十六进制表示为 4C
9D 39，其中第二个字节为非 ASCII 编码，需要增加等号，增加后对应的 ASCII 值为 L=9D9，则最后的 ASCII 编码为 4C 3D 39 44 39。解得此题。

答案 01001100 00111101 00111001 01000100 00111001。

编码开销 = （5-3）/3 = 66.7% 。

6-29 电子邮件系统需要将人们的电子邮件地址编成目录以便于查找。要建立这种目录应将人名划分为几个标准部分（例如，姓、名）。若要形成一个国际标准，那么必须解决哪些问题？

答：非常困难。人名的书写方法，例如，很多国家是先写名再写姓，但中国或日本等国家则先写姓再写名。有些国家的一些人还有中间的名。称呼也有非常多的种类，还有各式各样的头衔等，很难有统一的格式。

6-30 电子邮件系统使用 TCP 传送邮件。为什么有时我们会遇到邮件发送失败的情况？为什么有时对方会收不到我们发送的邮件？

答：有时对方的邮件服务器不工作，邮件就发送不出去。对方的邮件服务器出故障也会使邮件丢失。

6-31 基于万维网的电子邮件系统有什么特点？在传送邮件时使用什么协议？

答：

特点：不管在什么地方，只要能上网，在打开万维网浏览器后，就可以收发电子邮件。这时，邮件系统中的用户代理就是普通的万维网。

电子邮件从 A 发送到网易邮件服务器是使用 HTTP 协议。

两个邮件服务器之间的传送使用 SMTP。

邮件从新浪邮件服务器传送到 B 是使用 HTTP 协议。

6-32 DHCP 协议用在什么情况下？当一台计算机第一次运行引导程序时，其 ROM 中有没有该主机的 IP 地址、子网掩码或某个域名服务器的 IP 地址？

答：

动态主机配置协议 DHCP 提供了即插即用连网的机制。

这种机制允许一台计算机加入新的网络和获取 IP 地址而不用手工参与。

6-33 什么是网络管理？为什么说网络管理是当今网络领域中的热门课题？

答：网络管理简称网管，包括对硬件、软件和人力的使用、综合与协调，以便对网络资源进行监视、测试、配置、分析、评估和控制，以合理的价格满足网络使用需求，如实时运行性能、服务质量等。

网络是当今不可或缺的信息基础设施，尤其是进入互联网时代，网络变得越来越庞大，也越来越复杂。网络是一个由许多运行着多种协议的结点组成的分布式系统，这些结点需要相互通信和交换信息，网络的状态也总是不断变化着。为了上面提到的网络管理目标，必须依靠网络自身来对网络实现智能的高效管理，因此网络管理业成为网络技术必不可少的一个分支，也是网络领域中最热门的话题之一。

6-34 解释下列术语：网络元素、被管对象、管理进程、代理进程和管理信息库。

答：网络元素是指网络中的被管设备，有时简称网元，可以是主机、路由器、网桥、交换机/集线器、打印机、调制解调器等设备。

每一个网络设备可以有多个被管对象，可以是设备中的一个硬件部件（如一块网卡），业可以是某些硬件或软件（如路由选择协议）的配置参数集合。管理信息库是一个网络中所有被管对象的集合的数据结构。

管理站是整个网络管理系统的核心，管理站中的核心构件是管理程序，管理程序运行时会创建一个或若干个管理进程。

在每一个被管设备中都要运行一个网络管理的代理程序，运行时就成了代理进程。

一个综合网络管理系统包含 OSI 网络管理模型的多个或全部功能域。目前有的综合网络管理系统（如 CA 公司的 Unicenter、HP 的 OpenView、IBM 的 Tivoli）还涉及信息管理、存储管理等各种资源管理。

6-35 SNMP 使用 UDP 传送报文。为什么不使用 TCP？

答：因为 SNMP 协议采用客户/服务器工作方式，客户与服务器使用 request 和 response 报文建立了一种可靠的请求/响应关系，因此不必再耗时建立 TCP 连接。而采用首部开销比 TCP 小的 UDP 报文形式。

6-36 为什么 SNMP 的管理进程使用探询掌握全网状态属于正常情况，而代理进程用陷阱向管理进程报告属于较少发生的异常情况？

答：探询主要由管理站根据需要来向代理请求信息或要求代理执行某个动作，该方式开销和时延都相对大一些，再正常情况下，这些都是可以接受的。

尽管探询方式也可以为代理进程所用，但在严重异常情况下，需要及时地向管理进程报告。因此采用了陷阱方式。

6-37 SNMP 使用哪几种操作？SNMP 在 Get 报文中设置了请求标识符字段，为什么？

答：SNMP 有两种操作：(1)“读”操作，用 get 报文来检测各被管对象的状况。（2）“写”操作，用 set 报文来改变各被管对象的状况。

因为 SNMP 在 get 报文中设置请求标识符字段，可以允许管理进程同时向许多代理发送请求，代理响应回答的 get-response 报文中也包含相应的请求标识符，以区分不同的代理发回的响应报文。

6-38 什么是管理信息库 MIB？为什么要使用 MIB？

答:管理信息库 MIB 是一个网络中所有可能的被管对象集合的数据结构。

只有在 MIB 中的对象才是 SNMP 能够管理的。MIB 的定义与具体的网络管理协议无关，这对于厂商和用户都有利，厂商可以在产品中包含 SNMP 代理软件，并保证在定义新的 MIB 项目后该软件仍能够遵守标准。用户可以使用同一网络管理客户软件来管理具有不同版本的 MIB 的多个路由器。

6-39 什么是管理信息结构 SMI？它的作用是什么？

答:管理信息结构 SMI 是 SNMP 的另一个重要组成部分。SMI 标准指明了所有的 MIB 变量必须使用抽象语法记法 1（ASN.1）来定义。

6-40 用 ASN.1 基本编码规则对以下 4 个数组（SEQUENCE-OF）进行编码。假定每一个数字占用 4 个字节。

2345，1236，122，1236

答:整个的编码为：

```
30 18
   02 04 00 00 09 29
   02 04 00 00 04 D4
   02 04 00 00 00 7A
   02 04 00 00 04 D4
```

6-41SNMP 要发送一个 GetRequest 报文，以便向一个路由器获取 ICMP 的 icmpInParmProbs 的值。在 icmp 中变量 icmpInParmProbs 的标号是（5），它是一个计数器，用来统计收到的类型为参数问题的 ICMP 差错报告报文的数目。试给出这个 GetRequest 报文的编码。

答:1.3.6.1.2.1.5.5.0

```
30 29
   02 01 00
   04 06 70 75 62 6C 69 63
   A0 1C
      02 04 00 01 06 14
      02 01 00
      02 01 00
      30 0E
      30 0C
         06 08 2B 06 01 02 01 05 05 00
         05 00
```

6-42 对 tcp 的 OBJECT IDENTIFIER 是什么？

答: {1.3.6.1.2.1.6}

6-43 在 ASN.1 中，IP 地址（IPAddress）的类别是应用类。若 IPAddress=131.21.14.2，试求其 ASN.1 编码。

答：40 04 83 15 0E 02

6-44 什么是应用编程接口 API？它是应用程序和谁的接口？

答：当某个应用进程启动系统调用时，控制权就从应用进程传递给了系统调用接口。此接口再将控制权传递给计算机的操作系统，操作系统将此调用给某个内部过程，并执行所请求的操作。内部过程一旦执行完毕，控制权就又通过系统调用接口返回给应用程序。只要应用进程需要从操作系统获得服务，就要将控制权传递给操作系统，操作系统在执行必要的操作后将控制权返回给应用进程，这种系统调用接口又称为应用编程接口 API。API 是应用程序和操作系统之间的接口。

6-45 试举出常用的几种系统调用的名称，说明它们的用途。

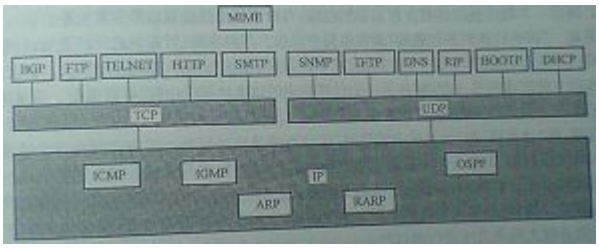
答： 无答案

6-46 图表示了各应用协议在层次中的位置。

（1）简单讨论一下为什么有的应用层协议要使用 TCP 而有的却要使用 UDP？

（2）为什么 MIME 画在 SMTP 之上？

（3）为什么路由选择协议 RIP 放在应用层？



答：（1）应用层协议根据各自功能的需求，有的需要使用面向连接的 TCP 服务，提供可靠的数据传输服务，如 FTP，HTTP 等；而有的协议使用无连接的 UDP 服务，提供比较灵活的服务，如 DHCP，SNMP 等。

（2）MIME 协议是扩展了的 SMTP 协议，是基于 SMIP 的，所以要放在 SMTP 上画。

（3）由于 RIP 协议是基于 UDP 协议而创建的。所以 RIP 协议应该放在 UDP 协议的上一层，即应用层协议。

第 7 章 网络安全

7-01 计算机网络都面临哪几种威胁？主动攻击和被动攻击的区别是什么？对于计算机网络的安全措施都有哪些？

答：计算机网络面临以下的四种威胁：截获（interception），中断(interruption)，篡改(modification),伪造（fabrication）。

网络安全的威胁可以分为两大类：即被动攻击和主动攻击。

主动攻击是指攻击者对某个连接中通过的 PDU 进行各种处理。如有选择地更改、删除、延迟这些 PDU。甚至还可将合成的或伪造的 PDU 送入到一个连接中去。主动攻击又可进一步划分为三种，即更改报文流；拒绝报文服务；伪造连接初始化。

被动攻击是指观察和分析某一个协议数据单元 PDU 而不干扰信息流。即使这些数据对攻击者来说是不易理解的，它也可通过观察 PDU 的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究 PDU 的长度和传输的频度，以便了解所交换的数据的性质。这种被动攻击又称为通信量分析。

还有一种特殊的主动攻击就是恶意程序的攻击。恶意程序种类繁多，对网络安全威胁较大的主要有以下几种：计算机病毒；计算机蠕虫；特洛伊木马；逻辑炸弹。

对付被动攻击可采用各种数据加密动技术，而对付主动攻击，则需加密技术与适当的鉴别技术结合。

7-02 试解释以下名词：（1）重放攻击；（2）拒绝服务；（3）访问控制；（4）流量分析；（5）恶意程序。

答：（1）重放攻击：所谓重放攻击（replay attack）就是攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程。

（2）拒绝服务：DoS(Denial of Service)指攻击者向因特网上的服务器不停地发送大量分组，使因特网或服务器无法提供正常服务。

（3）访问控制：（access control）也叫做存取控制或接入控制。必须对接入网络的权限加以控制，并规定每个用户的接入权限。

（4）流量分析：通过观察 PDU 的协议控制信息部分，了解正在通信的协议实体的地址和身份，研究 PDU 的长度和传输的频度，以便了解所交换的数据的某种性质。这种被动攻击又称为流量分析（traffic analysis）。

（5）恶意程序：恶意程序（rogue program）通常是指带有攻击意图所编写的一段程序。

7-03 为什么说，计算机网络的安全不仅仅局限于保密性？试举例说明，仅具有保密性的计算机网络不一定是安全的。

答：计算机网络安全不仅仅局限于保密性，但不能提供保密性的网络肯定是不安全的。网络的安全性机制除为用户提供保密通信以外，也是许多其他安全机制的基础。例如，存取控制中登陆口令的设计。安全通信协议的设计以及数字签名的设计等，都离不开密码机制。

7-04 密码编码学、密码分析学和密码学都有哪些区别？

答：密码学(cryptology)包含密码编码学(Cryptography)与密码分析学(Cryptanalytics)两部分内容。

密码编码学是密码体制的设计学,是研究对数据进行变换的原理、手段和方法的技术和

科学，而密码分析学则是在未知密钥的情况下从密文推演出明文或密钥的技术。是为了取得秘密的信息， 而对密码系统及其流动的数据进行分析，是对密码原理、手段和方法进行分析、攻击的技术和科学。

7-05 “无条件安全的密码体制”和“在计算上是安全的密码体制”有什么区别？

答：如果不论截取者获得了多少密文，但在密文中都没有足够的信息来惟一地确定出对应的明文，则这一密码体制称为无条件安全的，或称为理论上是不可破的。

如果密码体制中的密码不能被可使用的计算资源破译，则这一密码体制称为在计算上是安全的。

7-06 破译下面的密文诗。加密采用替代密码。这种密码是把 26 个字母（从 a 到 z）中的每一个用其他某个字母替代（注意，不是按序替代）。密文中无标点符号。空格未加密。

Kfd ktbd fzm eubd kfd pzyiom mztx ku kzyg ur bzha kfthcm ur mfudm zhx
Mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm zhx pfa kfd mdz tm sutythc
Fuk zhx pfdkfdi ntcm fzld pthcm sok pztk z stk kfd uamkdim eitdx sdruid
Pd fzld uoi efzk rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk
Hu foiia mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

答：单字母表是：

明文：a b c d e f g h I j k l m
密文：z s e x d r c f t g y b
明文：n o p q r s t u v w x y z
密文：h u n I m k o l p k a

根据该单字母表，可得到下列与与本题中给的密文对应的明文：

the time has come the walrus said to talk of many things
of shoes amd ships and sealing wax of cabbages and kings
and why the sea is boiling hot and whether pigs have wings
but wait a bit the oysters cried before we have our chat
for some of us are out of breath and all of us are fat
no hurry said the carpenter they thanked him much for that

7-07 对称密钥体制与公钥密码体制的特点各如何？各有何优缺点？

答：在对称密钥体制中，它的加密密钥与解密密钥的密码体制是相同的，且收发双方必须共享密钥，对称密码的密钥是保密的，没有密钥，解密就不可行，知道算法和若干密文不足以确定密钥。公钥密码体制中，它使用不同的加密密钥和解密密钥，且加密密钥是向公众公开的，而解密密钥是需要保密的，发送方拥有加密或者解密密钥，而接收方拥有另一个密钥。

两个密钥之一也是保密的，无解密密钥，解密不可行，知道算法和其中一个密钥以及若干密文不能确定另一个密钥。

优点：对称密码技术的优点在于效率高，算法简单，系统开销小，适合加密大量数据。对称密钥算法具有加密处理简单，加解密速度快，密钥较短，发展历史悠久等优点。

缺点：对称密码技术进行安全通信前需要以安全方式进行密钥交换，且它的规模复杂。公钥密钥算法具有加解密速度慢的特点，密钥尺寸大，发展历史较短等特点。

7-08 为什么密钥分配是一个非常重要但又十分复杂的问题？试举出一种密钥分配的方法。

答：密钥必须通过最安全的通路进行分配。可以使用非常可靠的信使携带密钥非配给互相通信的各用户，多少用户越来越多且网络流量越来越大，密钥跟换过于频繁，派信使的方法已不再适用。

举例：公钥的分配，首先建立一个值得信赖的机构（认证中心 CA），将公钥与其对应的实体进行绑定，每个实体都有 CA 发来的证书，里面有公钥及其拥有者的标识信息，此证书被 CA 进行了数字签名，任何用户都可从可信的地方获得 CA 的公钥，此公钥可用来验证某个公钥是否为某个实体所拥有。

7-09　公钥密码体制下的加密和解密过程是怎么的？为什么公钥可以公开？如果不公开是否可以提高安全性？

答：加密和解密过程如下：

（1）、密钥对产生器产生出接收者的一对密钥：加密密钥和解密密钥；

（2）、发送者用接受者的公钥加密密钥通过加密运算对明文进行加密，得出密文，发送给接受者 ；接受者用自己的私钥解密密钥通过解密运算进行解密，恢复出明文；

因为无解密密钥，解密是不可行的，所以公钥可以公开，知道算法和其中一个密钥以及若干密文不能确定另一个密钥。

7-10　试述数字签名的原理

答：数字签名采用了双重加密的方法来实现防伪、防赖。其原理为： 被发送文件用 SHA 编码加密产生 128bit 的数字摘要。然后发送方用自己的私用密钥对摘要再加密，这就形成了数字签名。将原文和加密的摘要同时传给对方。对方用发送方的公共密钥对摘要解密，同时对收到的文件用 SHA 编码加密产生又一摘要。将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。如两者一致，则说明传送过程中信息没有被破坏或篡改过。否则不然。

7-11　为什么需要进行报文鉴别？鉴别和保密、授权有什么不同？报文鉴别和实体鉴别有什么区别？

答：(1)使用报文鉴别是为了对付主动攻击中的篡改和伪造。当报文加密的时候就可以达到报文鉴别的目的，但是当传送不需要加密报文时，接收者应该能用简单的方法来鉴别报文的真伪。

(2)鉴别和保密并不相同。鉴别是要验证通信对方的确是自己所需通信的对象，而不是其他的冒充者。鉴别分为报文鉴别和实体鉴别。授权涉及到的问题是：所进行的过程是否被允许(如是否可以对某文件进行读或写)。

(3)报文鉴别和实体鉴别不同。报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。

7-12　试述实现报文鉴别和实体鉴别的方法。

答：(1)报文摘要 MD 是进行报文鉴别的简单方法。A 把较长的报文 X 经过报文摘要算法运算后得出很短的报文摘要 H。然后用自己的私钥对 H 进行 D 运算，即进行数字签名。得出已签名的报文摘要 D(H)后，并将其追加在报文 X 后面发送给 B。B 收到报文后首先把已签名的 D(H)和报文 X 分离。然后再做两件事。第一，用 A 的公钥对 D(H)进行 E 运算，得出报文摘要 H。第二，对报文 X 进行报文摘要运算，看是否能够得出同样的报文摘要 H。如一样，就能以极高的概率断定收到的报文是 A 产生的。否则就不是。

(2)A 首先用明文发送身份 A 和一个不重数 R_A 给 B。接着，B 响应 A 的查问，用共享的密

钥 K_{AB} 对 R_A 加密后发回给 A，同时也给出了自己的不重数 R_B。最后，A 再响应 B 的查问，用共享的密钥 K_{AB} 对 R_B 加密后发回给 B。由于不重数不能重复使用，所以 C 在进行重放攻击时无法重复使用是哟截获的不重数。

7-13 报文的保密性与完整性有何区别？什么是 MD5？

答：(1)报文的保密性和完整性是完全不同的概念。

保密性的特点是：即使加密后的报文被攻击者截获了，攻击者也无法了解报文的内容。

完整性的特点是：接收者接收到报文后，知道报文没有被篡改或伪造。

(2)MD5 是[RFC1321]提出的报文摘要算法，目前已获得了广泛的应用。它可以对任意长的报文进行运算，然后得出 128bit 的 MD 报文摘要代码。算法的大致过程如下：

①先将任意长的报文按模 2^{64} 计算其余数(64bit)，追加在报文的后面。这就是说，最后得出的 MD5 代码已包含了报文长度的信息。

②在报文和余数之间填充 1~512bit，使得填充后的总长度是 512 的整数倍。填充比特的首位是 1，后面都是 0。

③将追加和填充的报文分割为一个个 512bit 的数据块，512bit 的报文数据分成 4 个 128bit 的数据依次送到不同的散列函数进行 4 论计算。每一轮又都按 32bit 的小数据块进行复杂的运算。一直到最后计算出 MD5 报文摘要代码。

这样得出的 MD5 代码中的每一个比特，都与原来的报文中的每一个比特有关。

7-14 什么是重放攻击？怎样防止重放攻击？

答：(1)入侵者 C 可以从网络上截获 A 发给 B 的报文。C 并不需要破译这个报文(因为这可能很花很多时间)而可以直接把这个由 A 加密的报文发送给 B，使 B 误认为 C 就是 A。然后 B 就向伪装是 A 的 C 发送许多本来应当发送给 A 的报文。这就叫做重放攻击。

(2)为了对付重放攻击，可以使用不重数。不重数就是一个不重复使用的大随机数，即“一次一数”。

7-15 什么是“中间人攻击”？怎样防止这种攻击？

答：(1) 中间人攻击（Man-in-the-Middle Attack，简称“MITM 攻击”）是一种“间接”的入侵攻击， 这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。然后入侵者把这台计算机模拟一台或两台原始计算机，使“中间人”能够与原始计算机建立活动连接并允许其读取或篡改传递的信息，然而两个原始计算机用户却认为他们是在互相通信，因而这种攻击方式并不很容易被发现。所以中间人攻击很早就成为了黑客常用的一种古老的攻击手段，并且一直到今天还具有极大的扩展空间。

(2) 要防范 MITM 攻击，我们可以将一些机密信息进行加密后再传输，这样即使被“中间人”截取也难以破解，另外，有一些认证方式可以检测到 MITM 攻击。比如设备或 IP 异常检测：如果用户以前从未使用某个设备或 IP 访问系统，则系统会采取措施。还有设备或 IP 频率检测：如果单一的设备或 IP 同时访问大量的用户帐号，系统也会采取措施。更有效防范 MITM 攻击的方法是进行带外认证。

7－16 试讨论 Kerberos 协议的优缺点。

答：Kerberos 协议主要用于计算机网络的身份鉴别(Authentication)，其特点是用户只需输入一次身份验证信息就可以凭借此验证获得的票据(ticket-granting ticket)访问多个服务，即 SSO(Single Sign On)。由于在每个 Client 和 Service 之间建立了共享密钥，使得该协议具有相当的安全性。

概括起来说 Kerberos 协议主要做了两件事：Ticket 的安全传递； Session Key 的安全发布。

再加上时间戳的使用就很大程度上的保证了用户鉴别的安全性。并且利用 Session Key，在通过鉴别之后 Client 和 Service 之间传递的消息也可以获得 Confidentiality(机密性)，Integrity(完整性)的保证。不过由于没有使用非对称密钥自然也就无法具有抗否认性，这也限制了它的应用。不过相对而言它比 X.509 PKI 的身份鉴别方式实施起来要简单多了。

7－17 因特网的网络层安全协议族 Ipsec 都包含哪些主要协议？

答：在 Ipsec 中最主要的两个部分就是：鉴别首部 AH 和封装安全有效载荷 ESP。

AH 将每个数据报中的数据和一个变化的数字签名结合起来，共同验证发送方身份，使得通信一方能够确认发送数据的另一方的身份，并能够确认数据在传输过程中没有被篡改，防止受到第三方的攻击。它提供源站鉴别和数据完整性，但不提供数据加密。

ESP 提供了一种对 IP 负载进行加密的机制，对数据报中的数据另外进行加密，因此它不仅提供源站鉴别、数据完整性，也提供保密性。

IPSec 是 IETF（Internet Engineering Task Force，Internet 工程任务组）的 IPSec 小组建立的一套安全协作的密钥管理方案，目的是尽量使下层的安全与上层的应用程序及用户独立，使应用程序和用户不必了解底层什么样的安全技术和手段，就能保证数据传输的可靠性及安全性。

IPSec 是集多种安全技术为一体的安全体系结构，是一组 IP 安全协议集。IPSec 定义了在网际层使用的安全服务，其功能包括数据加密、对网络单元的访问控制、数据源地址验证、数据完整性检查和防止重放攻击。

7-18 试简述 SSL 和 SET 的工作过程。

答：首先举例说明 SSL 的工作过程。假定 A 有一个使用 SSL 的安全网页，B 上网时用鼠标点击到这个安全网页的链接。接着，服务器和浏览器就进行握手协议，其主要过程如下。

（1）浏览器向服务器发送浏览器的 SSL 版本号和密码编码的参数选择。

（2）服务器向浏览器发送服务器的 SSL 版本号、密码编码的参数选择及服务器的证书。证书包括服务器的 RSA 分开密钥。此证书用某个认证中心的秘密密钥加密。

（3）浏览器有一个可信赖的 CA 表，表中有每一个 CA 的分开密钥。当浏览器收到服务器发来的证书时，就检查此证书是否在自己的可信赖的 CA 表中。如不在，则后来的加密和鉴别连接就不能进行下去；如在，浏览器就使用 CA 的公开密钥对证书解密，这样就得到了服务器的公开密钥。

（4）浏览器随机地产生一个对称会话密钥，并用服务器的分开密钥加密，然后将加密的会话密钥发送给服务器。

（5）浏览器向服务器发送一个报文，说明以后浏览器将使用此会话密钥进行加密。然后浏览器再向服务器发送一个单独的加密报文，表明浏览器端的握手过程已经完成。

（6）服务器也向浏览器发送一个报文，说明以后服务器将使用此会话密钥进行加密。然后服务器再向浏览器发送一个单独的加密报文，表明服务器端的握手过程已经完成。

（7）SSL 的握手过程到此已经完成，下面就可开始 SSL 的会话过程。

下面再以顾客 B 到公司 A 用 SET 购买物品为例来说明 SET 的工作过程。这里涉及到两个银行，即 A 的银行（公司 A 的支付银行）和 B 的银行（给 B 发出信用卡的银行）。

（1）B 告诉 A 他想用信用卡购买公司 A 的物品。

（2）A 将物品清单和一个唯一的交易标识符发送给 B。

（3）A 将其商家的证书，包括商家的公开密钥发送给 B。A 还向 B 发送其银行的证书，包括

银行的公开密钥。这两个证书都用一个认证中心 CA 的秘密密钥进行加密。
（4）B 使用认证中心 CA 的公开密钥对这两个证书解密。
（5）B 生成两个数据包：给 A 用的定货信息 OI 和给 A 的银行用的购买指令 PI。
（6）A 生成对信用卡支付请求的授权请求，它包括交易标识符。
（7）A 用银行的公开密钥将一个报文加密发送给银行，此报文包括授权请求、从 B 发过来的 PI 数据包以及 A 的证书。
（8）A 的银行收到此报文，将其解密。A 的银行要检查此报文有无被篡改，以及检查在授权请求中的交易标识符是否与 B 的 PI 数据包给出的一致。
（9）A 的银行通过传统的银行信用卡信道向 B 的银行发送请求支付授权的报文。
（10）一旦 B 的银行准许支付，A 的银行就向 A 发送响应（加密的）。此响应包括交易标识符。　　（11）若此次交易被批准，A 就向 B 发送响应报文。

7-19　电子邮件的安全协议 PGP 主要都包含哪些措施？

答：PGP 是一种长期得到广泛使用和安全邮件标准。PGP 是 RSA 和传统加密的杂合算法，因为 RSA 算法计算量大，在速度上不适合加密大量数据，所以 PGP 实际上并不使用 RSA 来加密内容本身，而是采用 IDEA 的传统加密算法。PGP 用一个随机生成密钥及 IDEA 算法对明文加密，然后再用 RSA 算法对该密钥加密。收信人同样是用 RSA 解密出这个随机密钥，再用 IDEA 解密邮件明文。

7-20　路加密与端到端加密各有何特点？各用在什么场合？

答：（1）链路加密

优点：某条链路受到破坏不会导致其他链路上传送的信息被析出，能防止各种形式的通信量析出；不会减少网络系统的带宽；相邻结点的密钥相同，因而密钥管理易于实现；链路加密对用户是透明的。

缺点：中间结点暴露了信息的内容；仅仅采用链路加密是不可能实现通信安全的；不适用于广播网络。

（2）端到端加密

优点：报文的安全性不会因中间结点的不可靠而受到影响；端到端加密更容易适合不同用户服务的要求，不仅适用于互联网环境，而且同样也适用于广播网。

缺点：由于 PDU 的控制信息部分不能被加密，所以容易受到通信量分析的攻击。同时由于各结点必须持有与其他结点相同的密钥，需要在全网范围内进行密钥管理和分配.

为了获得更好的安全性，可将链路加密与端到端加密结合在一起使用。链路加密用来对 PDU 的目的地址进行加密，而端到端加密则提供了对端到端数据的保护。

7-21　试述防火墙的工作原理和所提供的功能。什么叫做网络级防火墙和应用级防火墙？

答：防火墙的工作原理：防火墙中的分组过滤路由器检查进出被保护网络的分组数据，按照系统管理员事先设置好的防火墙规则来与分组进行匹配，符合条件的分组就能通过，否则就丢弃。

防火墙提供的功能有两个：一个是阻止，另一个是允许。阻止就是阻止某种类型的通信量通过防火墙。允许的功能与阻止的恰好相反。不过在大多数情况下防火墙的主要功能是阻止。

网络级防火墙：主要是用来防止整个网络出现外来非法的入侵，属于这类的有分组过滤和授权服务器。前者检查所有流入本网络的信息，然后拒绝不符合事先制定好的一套准则的数据，而后者则是检查用户的登录是否合法。

应用级防火墙：从应用程序来进行介入控制。通常使用应用网关或代理服务器来区分各种应用。

第 8 章 因特网上的音频/视频服务

8-1 音频/视频数据和普通文件数据都有哪些主要区别？这些区别对音频/视频数据在因特网上传送所用的协议有哪些影响？既然现有的电信网能够传送音频/视频数据，并且能够保证质量，为什么还要用因特网来传送音频/视频数据呢？

答：

区别

第一，多音频/视频数据信息的信息量往往很大，

第二，在传输音频/视频数据时，对时延和时延抖动均有较高的要求。

影响

如果利用 TCP 协议对这些出错或丢失的分组进行重传，那么时延就会大大增加。因此实时数据的传输在传输层就应采用用户数据报协议 UDP 而不使用 TCP 协议。

电信网的通信质量主要由通话双方端到端的时延和时延抖动以及通话分组的丢失率决定。这两个因素都是不确定的，因而取决于当时网上的通信量，有网络上的通信量非常大以至于发生了网络拥塞，那么端到端的网络时延和时延抖动以及分组丢失率都会很高，这就导致电信网的通信质量下降。

8-2 端到端时延与时延抖动有什么区别？产生时延抖动的原因时什么？为什么说在传送音频/视频数据时对时延和时延抖动都有较高的要求？

答：端到端的时延是指按照固定长度打包进 IP 分组送入网络中进行传送；接收端再从收到的 IP 包中恢复出语音信号，由解码器将其还原成模拟信号。时延抖动是指时延变化。数据业务对时延抖动不敏感，所以该指标没有出现在 Benchmarking 测试中。由于 IP 上多业务，包括语音、视频业务的出现，该指标才有测试的必要性。

产生时延的原因

IP 数据包之间由于选择路由不同，而不同路由间存在不同时延等因素，导致同一 voip 的数据包之间会又不同的时延，由此产生了时延抖动。

把传播时延选择的越大，就可以消除更大的时延抖动，但所要分组经受的平均时延也增大了，而对某些实时应用是很不利的。如果传播时延太小，那么消除时延抖动的效果就较差。因此播放时延必须折中考虑。

8-3 目前有哪几种方案改造因特网使因特网能够适合于传送/音频视频数据？

答： 1.大量使用光缆，是网络的时延和时延抖动减小，使用具有大量高速缓存的高数路由器，在网上传送实时数据就不会有问题。

2.将因特网改造为能够对端到端的带宽实现预留，从而根本改变因特网的协议栈—从无连接的网络变为面向连接的网络。

3.部分改动因特网的协议，也能够使多媒体信息在因特网上的传输质量得到改进。

8-4 实时数据和等时数据是一样的意思吗？为什么说因特网是不等时的？实时数据都有哪些特点？试说播放延时的作用？

答： 实时数据和等时数据不是一样的意思。

模拟的音频/视频信号只有经过数字化以后才能在因特网上传送。就是对模拟信号

要经过采样和模数转换为数字信号，然后将一定数量的比特组组装成分组进行传送。这些分组在发送时的时间间隔时恒定的，但传统的因特网本身是非等时的。这是因为在时延 IP 协议的因特网中，每一个分组是独立的传送，因而这些分组在到达接收端时就变成非等时的。

消除时延的抖动。

8-5 流式存储音频/视频，流式实况音频/视频和交互式音频/视频都有何区别？

答：　流式存储音频/视频是边下载边播放，即在文件下载后不久就开始播放。

流式实况音频/视频是发送时边录制边发送，接受时也是能够连续播放。接受方收到的节目时间和节目中事件的发生时间可以认为是同时的。

交互式音频/视频是用户使用因特网和其他人进行交互式通信。

8-6 媒体播放器和媒体服务器的功能是什么？请用例子说明。媒体服务器为什么称为流式服务器？

答：　媒体播放器的主要功能是：管理用户界面，解压缩，消除时延抖动和处理传输带来的差错。

媒体服务器的主要功能是使用元文件的 URL 接入到媒体服务器，请求下载浏览器所请求的音频/视频文件，给出响应把该音频/视频文件发送给媒体播放器。

8-7 实时流式协议 RTSP 的功能是什么？为什么说它是个带外协议？

答：　RTSP 是 IETF 的 MMUSIC 工作组开发的协议，功能是为了给流式过程增加更多的功能而设计的协议。

RTSP 本身并不传送数据，而仅仅是使媒体播放器能够控制多媒体的传送，因此 RTSP 又称为外带协议。

8-08 狭义的 IP 电话和广义的 IP 电话都有哪些区别？IP 电话都有哪几种连接方式？

答：狭义的 IP 电话就是指在网络上打电话。广义的 IP 电话不仅仅是电话通信，而且还可以是在 IP 网络上进行交互式多媒体实时通信（包括电话.视像等）甚至还包括即时传信 IM。IP 电话有 3 种连接方式分别为：（1）2 个 PC 机之间的通话。（2）PC 机到固定用户之间的通话。（3）2 个固定电话之间打 IP 电话。

8-09 IP 电话的通话质量与那些因素有关？影响 IP 电话话音质量的主要因素有哪些？为什么 IP 电话的通话质量是不确定的？

答：IP 电话的通话质量主要由两个因素决定。一是通话双方端到端的时延和时延抖动，另一个是话音分组的丢失率。影响 IP 电话话音质量主要因素有：语音编解码技术、包丢失以及时延和时延抖动等。若网络上的通信量非常大以致发生了网络拥堵，那么端到端时延和时延抖动以及分组丢失率都会很高，这就导致 IP 电话的通信质量下降。因此，一个用户使用 IP 电话的通信质量取决于当时其他的许多用户的行为。

8-10 为什么 RTP 协议同时具有运输层和应用层的特点？

答：从开发者的角度看，RTP 应当是应用层的一部分。在应用程序的发送端，开发者必须编写用 RTP 封装分组的程序代码，然后把 RTP 分组交给 UDP 套接字接口。在接受端，RTP 分组通过 UDP 套接字接口进入应用层后。还要利用开发者编写的程序代码从分组中把应用数据块提取出来。然而 RTP 的名称又隐含地表示出它是一个运输层协议。这样划分也是可以的，应为 RTP 封装了多媒体应用的数据块，并且由于 RTP 向多媒体应用程序提供了服务（如时间戳

和序号）。因此可以吧 RTP 看成是在 UDP 之上的一个运输层子层的协议。

8-11 RTP 协议能否提供应用分组的可靠传输？请说明理由。

答：不能。因为 RTP 为实时应用提供端到端的运输，但不提供任何服务质量的保证。RTP 是一个协议框架因为它只包含了实时应用的一些共同功能。RTP 并不对多媒体数据块做任何处理而只是向应用层提供一些附加的信息，让应用层知道应当如何进行处理。

8-12 在 RTP 的分组中为什么要使用序号、时间戳和标记？

答：序号占 16 位。对每一个发送出的 RTP 分组，其序号加 1.在一次 RTP 会话开始时的初始序号是随机选择的序号使接收端能够发现丢失的分组，同时也能够将失序的 RTP 分组重新按序排列好。时间戳反映了 RTP 分组中的数据的第一字节的采样时刻。接收端使用时间戳克准确的知道应当在什么时间还原哪一个数据块，从而消除时间的抖动。时间戳还可用来使视频应用中声音和图像的同步。标记置 1 表示这个 RTP 分组具有特殊意义。

8-13 RTCP 协议使用在什么场合？它们各有何主要特点？

答：RTP 协议分别使用在：结束分组 BYE 表示关闭一个数据流；特定应用分组 APP 时应用程序能够定义新的分组类型；接收端报告分组 RR 用来使接收端周期性地向所有的点用多播方式进行报告；发送端报告分组 SR 用来使发送端周期性地向所有接收端用多播方式进行报告；远点描述分组 SDES 给出会话中参加者的描述。

8-14 IP 电话的两个主要标准各有何特点？

解：IP 电话的两个标准分别为：ITU-T 定义的 H.323 协议和 IETF 提出的绘画发起协议 SIP.

H.323 协议的特点：以已有的电路交换电话网为基础，增加了 IP 电话的功能。H.323 的指令沿用原有电话网的信令模式，与原有电话网的连接比较容易。

SIP 协议的特点：以英特网为基础，将 IP 电话视为英特网那个上的新应用。SIP 使用了 HTTP 的许多首部、编码规则、差错码以及一些鉴别机制。它比 H.323 具有更好的可扩缩性。

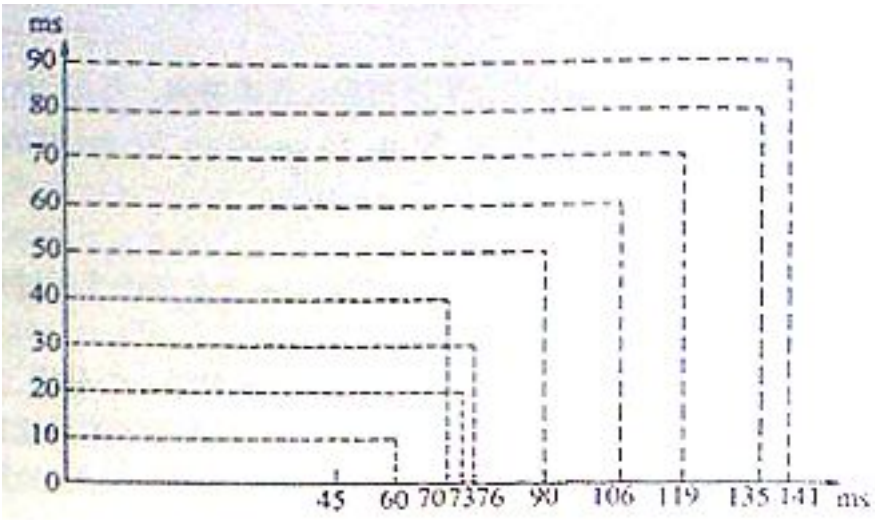
8-15 携带实时音频信号的固定长度分组序列发送到因特网。每隔 10ms 发送一个分组。前 10 个分组通过网络的时延分别为 45ms，50ms，53ms，46ms，30ms，40ms，46ms，49ms，55ms 和 51ms。

（1）用图表示出这些分组发出时间和到达时间。

（2）若在接收端还原时的端到端时延为 75ms，试求出每个分组经受的时延。

（3）画出接收端缓存中的分组数与时间的关系。

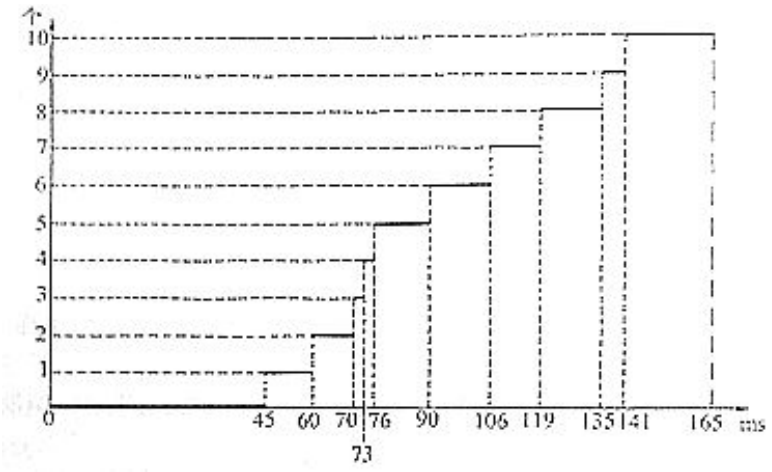
解： （1）下图（a）的纵横坐标表示这些分组的发出时间和到达时间



（a）分组发送时间和到达时间图

（2）每个分组经受的时延分别为：30，25，22，29，455，35，29，26，20 和 24ms

（3）接收端缓存中的分组数与时间的关系如下图（b）所示。



（b）接收端缓存中的分组数语时间关系图

8-16 话音信号的采样速率为 8000HZ，每隔 10ms 将已编码的话音采样装配为话音分组。每一个话音分组在发送之前要加上一个时间戳。假定时间戳是从一个时钟得到的，该时钟每隔△秒将计时器加 1.试问能否将△取为 9ms？如果行，请说明理由。如果不行，你认为△应取为多少？

解：不能将△取为 9ms，可以将△取为 5ms

8-17 在传送音频/视频数据时，接收端的缓存空间的上限由什么因素决定？实时数据流的数据率和时延抖动对缓存空间上限的确定有何影响？

解：接收端的缓存空间的上限取决于还原播放时所容许的时延，当还原播放时所用需的时延已经确定时，缓存空间的上限与实时数据流的数据率成正比。时延抖动越大，缓存空间也应越大。

8-18 什么是服务质量 QoS？为什么说“因特网根本没有服务质量可言”？

解：服务质量 QoS 是服务性能的总效果，此效果决定了一个用户对服务的满意程度。因特网

的网络本身提供的服务是不可靠的，它不能保证服务质量。实际上“尽最大努力交付”的服务就是没有质量保证的服务，根本没有服务质量可言。

8-19 在讨论服务质量时，管制、调度、呼叫接纳表示什么意思？

解：管制：使某个数据流不影响其他正常数据流在网络中通过的一种机制。

调度：路由器的队列所采用的排队规则。

呼叫接纳：数据流要事先声明它所需要的服务质量，然后或者被准许进入网络，或者被拒绝进入网络。

8-20 试比较先进先出（FIFO）排队、公平排队（FQ）和加权公平排队（WFQ）的优缺点。

解：先进先出（FIFO）排队的优点：实施简单；其缺点：不能区分时间敏感分组和一般数据分组，并且对排在长分组的短分组也不公平。

公平排队（FQ）的优点：在高优先级队列中总是有分组时，克服优先排队的局限，避免了低优先级队列的分组长期得不到服务的现象出现；其缺点：长分组得到的服务时间长，而短分组得到的服务时间短，并且没有区分分组的优先级。

加权公平排队（WFO）的优点：通过为每个队列分配一个与所需带宽百分比相对应的权重，使高优先级队列中的分组有更多的机会得到服务；其缺点：实施起来很复杂。

8-21 假定有一个支持三种类别的缓存运行加权公平排队 WFQ 调度算法,并假定这三种类别的权重分别是 0.5, 0.25, 0.25。如果是采用循环调度，那第这三个类别接受服务的顺序是 123123123…。

（1）如果每种类别在缓存中都有大量的分组，试问这三种类别的分组可能以何种顺序接受服务？

（2）如果第 1 类和第 3 类在缓存中有大量的分组，但缓存中没有第 2 类的分组，试问这两类分组可能以何种顺序接受服务？

解：（1）如果每种类别在缓存中都有大量的分组，这三种类别的分组接受服务的顺序有：112311231123…, 113211321132…, 211321132113…, 311231123112…, 231123112311…, 321132113211…。

（2）如果 1 类和第 3 类在缓存中有大量的分组，但缓存中没有第 2 类的分组，则这两类分组接受服务的顺序有：113113113…, 311311311。

8-22 漏桶管制器的工作原理是怎样的？数据流的平均速率、峰值速率和突发长度各表示什么意思？

解：漏桶管制器简称漏桶，它是一种抽象的机制。在漏桶中可装许多权标，但最多装入 b 个权标，只要漏桶中的权标数小于 b 个，新的权标就以每秒 r 个权标的恒定速率加入到漏桶中。但若漏桶已装了 b 个权标，则新的权标就不再装入，而漏桶的权标数达到最大值 b。

漏桶管制分组流进入网络的过程如下。分组进入网络前先要进入一个队列中等候漏桶中的权标，就可从漏桶取走一个权标，然后就准许一个分组从队列进入网络。若漏桶已无权标，就要等新的权标注入漏桶后，再把这个权标拿走后才能准许下一个分组进入网络。假定在时间间隔 t 中把漏桶中的全部 b 个权标都取走。但在这个时间间隔内漏桶又装入了 rt 个新权标，因此在任何时间间隔 t 内准许进入网络的分组数的最大值为 rt + b。控制权标进入漏桶的速率 r 就可对分组进入网络的速率进行管制。

平均速率　网络需要控制一个数据流的平均速率。这里的平均速率指的是在一定的时间间隔内通过的分组数。

峰值速率　峰值速率限制了数据流在非常短的时间间隔内的流量。

突发长度　网络也限制在非常的时间间隔内连续注入到网络中的分组数。

8-23　采用漏桶机制可以控制达到某一数值的、进入网络的数据率的持续时间。设漏桶最多可容纳 b 个权标。当漏桶中的权标小于 b 个时，新的权标就以每秒 r 个权标的恒定速率加入漏桶中。设分组进入网络的速率为 N pkt/s（pkt 代表分组），试推导以此速率进入网络所能持续的时间 T 。讨论一下为什么改变权标加入到漏桶中的速率就可以控制分组进入网络的速率。

解：假定在时间间隔 t 中把漏桶中的全部 b 个权标都取走。但在这个时间间隔内漏桶又装入了 rt 个新权标，因此在任何时间间隔 t 内准许进入网络的分组数的最大值为 rt + b。 T ＝（rt +b）/ N。控制权标进入漏桶的速率 r 就可对分组进入网络的速率进行管制。

8-24　在上题中，设 b = 250 token, r = 5000 token/s, N = 25000 pkt/s。试求分组用这样的速率进入网络持续多长时间。若 N ＝2500 pkt/s,　重新计算本题。

解：T ＝（rt + b）/ N = 0.21s

若 N ＝2500pkt/s,则 T ＝2.1s

8-25　试推导公式（8-2）。

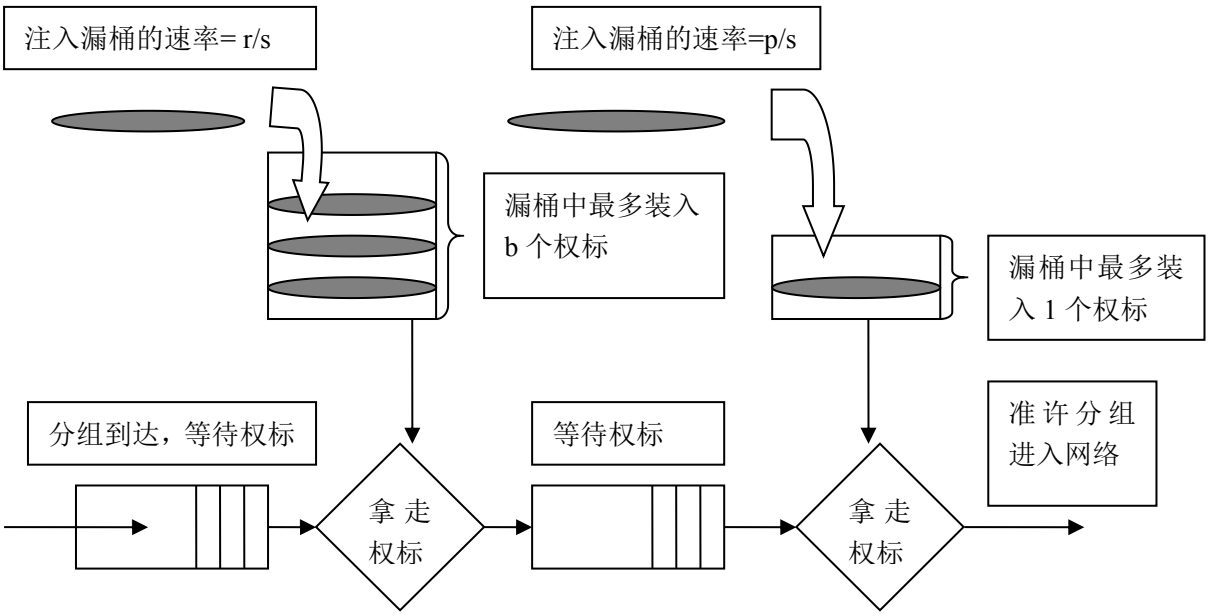
解：考虑分组 i。假定漏桶 i 已经装满了 bi 个权标。这就表示分组流 i 不需要等待就可以从漏桶中拿走 bi 个权标，因此 bi 个分组可以马上从路由器输出。但分组流 i 得到的数据率是由公式（8-1）给出。这 bi 个分组吵的最后一个分组所经受的时延最大，它等于这 bi 个分组所需的时间 dmax，dmax = bi / Ri =(bi∑wj) / (R×wi)。

8-26　假定图 8-22 中分组流 1 的漏桶权标装入速率 r1< Rw1/（∑wi），试证明：（8-2）式给出的 dmax 实际上是分组流 1 中任何分组在 WFQ 队列中所经受的最大时延。

解：r1<Rw1/(∑wi)，dmax = bi/ri,显然当 i=1 时，dmax 最大。

8-27 考虑 8.4.2 节讨论的管制分组流的平均速率和突发长度的漏桶管制器。现在我们限制其峰值速率为 p 分组/秒。试说明怎样把一个漏桶管制器的输出流入到第二个漏桶管制器的输入，以便用这样串接的两个漏桶能够管制分组流的平均速率、峰值速率以及突发长度。第二个漏桶的大小和权标产生的速率应当是怎样的？

解：如下图所示，第二个漏桶的大小是 1，权标产生的速率是 p/s。



8-28 综合服务 IntServ 由哪几个部分组成在？有保证的服务和受控负载的服务有何区别？

答：IntServ 共又以下四个组成部分：

（1）资源预留协议 RSVP，它是 IntServ 的信令协议。

（2）接纳控制（admission control），用来决定是否同意对某一资源的请求。

（3）分类器（classifier），用来把进入路由器的分组进行分类，并根据分类的结果把不同的类别的分组放入特定的队列。

（4）调度器（scheduler），根据服务质量要求决定分组发送的前后顺序。

有保证的服务和受控负载的服务的区别：

（1）有保证的服务（guaranteed service），可保证一个分组在通过路由器时的排队时延有一个严格的上限。

（2）受控负载的服务（controlled-load service），可以使应用程序得到比通常的“尽最大努力”更加可靠的服务。

8-29 试述资源预留协议 RSVP 的工作原理。

答：发送端依据高、低带宽的范围、传输迟延，以及抖动来表征发送业务。RSVP 从含有’业务类别(TSpec)’信息的发送端发送一个路径信息给目的地址(单点广播或多点广播的接收端)。每一个支持 RSVP 的路由器沿着下行路由建立一个’路径状态表’，其中包括路径信息里先前的源地址(例如，朝着发送端的上行的下一跳)为了获得资源预留，接收端发送一个上行的 RESV(预 留 请 求)消息。除了 TSpec，RESV 消息里有’请求类别(RSpec)，表明所要求的综合服务类型，还有一个’过虑器类别’，表征正在为分组预留资源(如传输协议和端口号)。RSpec 和过虑器类别合起来代表一个’流的描述符’，路由器就是靠它来识别每一个预留资源的 。

当每个支持 RSVP 的路由器沿着上行路径接收 RESV 的消息时，它采用输入控制过程证实请求，并且配置所需的资源。如果这个请求得不到满足(可能由于资源短缺或未通过认证)，路由器向接收端返回一个错误消息。如果这个消息被接受，路由器就发送上行 RESV 到下一

个 路 由 器

当最后一个路由器接收 RESV，同时接受请求的时候，它再发送一个证实消息给接收端。

当发送端或接收端结束了一个 RSVP 会话时，有一个明显的断开连接的过程。

8-30 区分服务 DiffServ 与综合服务 IntServ 有何区别？区分服务的工作原理是怎样的 ？

答：区分服务 DiffServ 与综合服务 IntServ 的区别：

（1） 区分服务 DiffServ 层次简单，伸缩性较好：DiffServ 工作范围分为两个层次：DS 域和 DS 区。DS 标记只是规定了有限数量的业务级别，状态信息的数量正比于业务级别，而不是流的数量。而综合服务 IntServ 伸缩性差，在 WAN 中，各种各样的子网会不断增多，并且随着流数目的增加，状态信息的数量成比例上升，重传 PATH 和 RESV 信息会占用大量的路由器存储空间和处理开销。

（2） 区分服务 DiffServ 便于实现：只在网络的边界上才需要复杂的分类、标记、管制和整形操作。ISP 核心路由器只需要实现行为聚集（BA）的分类，因此实现和部署区分、分级都比较容易。

（3） 区分服务 DiffServ 不影响路由：DiffServ 的节点提供服务的手段只限于队列调度和缓冲管理，并不涉及路由选择，而综合服务 Intserv 对现有路由器的改造十分复杂。由于需要进行端到端的资源预留，必须要求从发送到接收之间所有路由器都支持 RSVP 和许可控制协议，同时每个路由器还要花费大量的资源来维护和更新数据库

区分服务的工作原理：区分服务体系结构（DiffServ）定义了一种可以在互联网上实施可扩展的服务分类的体系结构。一种“服务”，是由在一个网络内，在同一个传输方向上，通过一条或几条路径传输数据包时的某些重要特征所定义的。这些特征可能包括吞吐率、时延、时延抖动，和/或丢包率的量化值或统计值等，也可能是指其获取网络资源的相对优先权。服务分类要求能适应不同应用程序和用户的需求，并且允许对互联网服务的分类收费。

DiffServ 体系结构由许多在网络节点上实现的功能要素组成，包括每一跳转发小集合，数据包归类功能，和交通调节功能。其中，交通调节功能又包含测量、标记、整形、和监察策略四部分。在本体系结构，只在网络的边界节点上实现复杂的分类和调节功能，并且，通过在 IPv4 和 IPv6 包头的 DS 段做适当的标记 [DSFIELD]，聚合流量，然后根据所做的标记，采取不同的每一跳转发策略。因此，本体系结构具备可扩展性。“每一跳行为”保证了在互相竞争资源的数据流中为每个网络节点分配缓冲区和带宽资源时，有一个合理的处理力度。在核心网络节点上，无需维护每个应用程序流或每个用户转发状态。

8-31 在区分服务 DiffServ 中的每跳行为 PHB 是什么意思？EF PHB 和 AF PHB 有何区别？它们个试用于什么样的通信量？

答：DiffServ 定义了在转发分组时体现服务水平的每跳行为 PHB。所谓“行为“就是指在转发分组时路由器对分组是怎样处理的。”每跳“是强调这里所说的行为只涉及到本路由器转发的这一跳的行为，而下一个路由器再怎样处理则与本路由器的处理无关。

EF PHB 和 AF PHB 的区别：

（1） EF 指明离开一个路由器的通信量的数据率必须等于或大于某一数值。因此 EFPHB 用来构造通过 DS 域的一个低丢失率、低时延、低时延抖动、确保带宽的端到端服务

（2） AF 用 DSCP 的第 0～2 位把通信量 划分为四个等级，并给每一种等级提供最低数量的带宽和缓存空间。对其中的每一个等级在用 DSCP 的第 3～5 位划分出三个“丢弃优先级“。当发生网络拥塞时，对于每一个等级的 AF，路由器就首先把”丢弃优先级“较高的分组丢弃。

8-32 假定一个发送端向 2^n 接收端发送多播数据流，而数据流的路径是一个完全的二叉树，在此二叉树的没有一个节点上都有一个路由器。若使用 RSVP 协议进行资源预留，问总共要产生多少个资源预留报文 RESV（有的在接收端产生，也有的在网络中的路由器产生）？

解： 按题意，此二叉树的叶节点有 2^n 个，故二叉树的深度为 n+1。每一个节点向其上游节点发送一个 RESV 报文，故总发送 $2^{n+1}-1$ 个 RESV 报文.

第 9 章 无线网络和移动网络

9-01．无线局域网都由哪几部分组成？无线局域网中的固定基础设施对网络的性能有何影响？接入点 AP 是否就是无线局域网中的固定基础设施？

答：无线局域网由无线网卡、无线接入点(AP)、计算机和有关设备组成，采用单元结构，将整个系统分成许多单元，每个单元称为一个基本服务组。

所谓“固定基础设施”是指预先建立起来的、能够覆盖一定地理范围的一批固定基站。直接影响无线局域网的性能。

接入点 AP 是星形拓扑的中心点，它不是固定基础设施。

9-02． Wi-Fi 与无线局域网 WLAN 是否为同义词？请简单说明一下。

答：Wi-Fi 在许多文献中与无线局域网 WLAN 是同义词。

802.11 是个相当复杂的标准。但简单的来说，802.11 是无线以太网的标准，它是使用星形拓扑,其中心叫做接入点 AP(Access Point),在 MAC 层使用 CSMA/CA 协议。凡使用 802.11 系列协议的局域网又称为 Wi-Fi(Wireless-Fidelity,意思是“无线保真度”)。因此，在许多文献中，Wi-Fi 几乎成为了无线局域网 WLAN 的同义词。

9-03 服务集标示符 SSID 与基本服务集标示符 BSSID 有什么区别？

答：SSID（Service Set Identifier）AP 唯一的 ID 码，用来区分不同的网络，最多可以有

32 个字符，无线终端和 AP 的 SSID 必须相同方可通信。无线网卡设置了不同的 SSID 就可以进入不同网络，SSID 通常由 AP 广播出来，通过 XP 自带的扫描功能可以相看当前区域内的 SSID。出于安全考虑可以不广播 SSID，此时用户就要手工设置 SSID 才能进入相应的网络。简单说，SSID 就是一个局域网的名称，只有设置为名称相同 SSID 的值的电脑才能互相通信。

BSS 是一种特殊的 Ad-hoc LAN 的应用，一个无线网络至少由一个连接到有线网络的 AP 和若干无线工作站组成，这种配置称为一个基本服务装置 BSS (Basic Service Set)。一群计算机设定相同的 BSS 名称，即可自成一个 group，而此 BSS 名称，即所谓 BSSID。

9-04. 在无线局域网中的关联（association）的作用是什么？

答：802.11 标准并没有定义如何实现漫游，但定义了一些基本的工具。例如，一个移动站若要加入到一个基本服务及 BSS，就必须先选择一个接入点 AP，并与此接入点建立关联（association）。建立关联就表示这个移动站加入了选定的 AP 所属子网，并和这个接入点 AP 之间粗昂见了一个虚拟线路。只有关联的 AP 才想这个移动站发送数据帧，而这个移动站也只有通过关联的 AP 才能向其他站点发送数据帧。这和手机开机之后必须和某个基站建立关联的概念是相似的。

9-05. 以下几种接入（固定接入、移动接入、便携接入和游牧接入）的主要特点是什么？

答：

接入方式	主要特点
固定接入	在作为网络用户期间，用户设置的地理位置保持不变
移动接入	用户设备能够以车辆熟读（一般取为每小时 120 公里）移动时进行网络通讯。当发生切换（即用户移动到不同蜂窝小区）时，通信仍然是连续的。
便携接入	在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力。
游牧接入	用户设备的地理位置至少在进行网络通信时保持不变。如果用户设备移动了位置（改变了蜂窝小区），那么再次进行通信时可能还要寻找最佳的基站。

9-06. 无线局域网的物理层主要有哪几种？

答：无线局域网的物理层主要有 802.11 家族谱、蓝牙新贵、家庭网络的 HomeRF

9-07. 无线局域网的 MAC 协议有哪些特点？为什么在无线局域网中不能使用 CSMA/CD 协议而必须使用 CSMA/CA 协议？

答：无线局域网的 MAC 协议提供了一个名为分布式协调功能（DCF）的分布式接入控制机制以及工作于其上的一个可选的集中式控制，该集中式控制算法称为点协调功能（PCF）。DCF 采用争用算法为所有通信量提供接入；PCF 提供无争用的服务，并利用了 DCF 特性来保证它的用户可靠接入。PCF 采用类似轮询的方法将发送权轮流交给各站，从而避免了冲突的产生，对于分组语音这样对于时间敏感的业务，就应提供 PCF 服务。 由于无线信

道信号强度随传播距离动态变化范围很大，不能根据信号强度来判断是否发生冲突，因此不适用有线局域网的的冲突检测协议 CSMA/CD。802.11 采用了 CSMA/CA 技术，CA 表示冲突避免。这种协议实际上是在发送数据帧前需对信道进行预约。 这种 CSMA/CA 协议通过 RTS（请求发送）帧和 CTS（允许发送）帧来实现。源站在发送数据前，先向目的站发送一个称为 RTS 的短帧，目的站收到 RTS 后向源站响应一个 CTS 短帧，发送站收到 CTS 后就可向目的站发送数据帧。

9-08．为什么无线局域网的站点在发送数据帧时，即使检测到信道空闲也仍然要等待一小段时间？为什么在发送数据帧的过程中不像以太网那样继续对信道进行检测？

答：因为电磁波在总线上总是以有限的速率传播的。无线局域网的站点在传送数据帧时，检测到信道空闲，其实并不空闲。数据在线路上还会出现碰撞，一旦出现碰撞，在这个帧的发送时间内信道资源都被浪费了，所以要等待一小段时间。

因为无线局域网上发送数据帧后要对方必须放回确认帧，以太网就不需要对方发回确认帧。

9-09．结合隐蔽站问题和暴露站问题说明 RTS 帧和 CTS 帧的作用。RTS/CTS 是强制使用还是选择使用？请说明理由。

答：源站在发送数据帧之前发送 RTS 帧，若信道空闲，则目的站响应 CTS 帧，当源站收到 CTS 帧后就可发送其数据帧，实际上就是在发送数据帧前先对信道预约一段时间。RTS/CTS 是选择使用的，因为当数据帧本身长度很短时，使用 RTS/CTS 反而会降低效率。

9-10．为什么在无线局域网上发送数据帧后要对方必须发回确认帧，而以太网就不需要对方发回确认帧？

答：无线局域网可能出现检测错误的情况：检测到信道空闲，其实并不空闲，而检测到信道忙，其实并不忙，因此需要接收方发回确认帧来确定信道是否空闲。

9-11．无线局域网的 MAC 协议中的 SIFS，PIFS 和 DIFS 的作用是什么？

答：SIFS，即短帧间间隔。SIFS 是最短的帧间间隔，用来分隔开属于一次对话的各帧；PIFS，即点协调功能帧间间隔（比 SIFS 长），是为了在开始使用 PCF 方式时（在 PCF 方式下使用，没有争用）优先获得接入到媒体中；DIFS，即分布协调功能帧间间隔（最长的 IFS），在 DCF 方式中用来发送数据帧和管理帧。

9-12．试解释无线局域网中的名词：BSS,ESS,AP,BSA,DCF,PCF 和 NAV.

答：BSS：一种非凡的 Ad-hoc LAN 的应用，称为 Basic Service Set (BSS)，一群计算机设定相同的 BSS 名称，即可自成一个 Group，而此 BSS 名称，即所谓 BSSID。

ESS：一种 infrastructure 的应用，一个或多个以上的 BSS，即可被定义成一个 Extended Service Set（ESS），使用者可于 ESS 上 Roaming 及存取 BSS 中的任何资料，其中 Access Points 必须设定相同的 ESSID 及 channel 才能允许 Roaming.

AP 接入点： 用于无线网络的无线 HUB，是无线网络的核心。它是移动计算机用户进入有线以太网骨干的接入点，AP 可以简便地安装在天花板或墙壁上，它在开放空间最大覆盖范围可达 300 米，无线传输速率可以高达 11Mbps。

BSA:一个基本服务集 BSS 所覆盖的地理范围。

DCF:分布协调功能，DCF 不采用任何中心控制，而是在每一个节点使用 CSMA 机制的分布式接入算法，让各个站通过争用信道来获取发送权。

PCF:点协调功能，PCF 是选项，是用接入点 AP 集中控制整个 BSS 内的活动，因此自组网

络就没有 PCF 子层。PCF 使用集中控制的接入算法，用类似于探询的方法把发送数据权轮流交给各个站，从而避免碰撞的产生。

NAV:网络分配向量指出了信道处于忙状态的持续时间,信道处于忙状态就表示:或者是由于物理层的载波监听检测到信道忙，或者是由于 MAC 层的虚拟载波监听机制指出了信道忙。

9-13．冻结退避计时器剩余时间的做法是为了使协议对所有站点更加公平，请进一步解释。

答：站点每经历一个时隙的时间就检测一次信道。这可能发生两种情况，若检测到信道空闲，退避计时器就继续倒计时，若检测到信道忙，就冻结退避计时器的剩余时间，重新等待信道变为空闲并经过时间 DIFS 后，从剩余时间开始继续倒计时。如果退避计时器的时间减小到零时，就开始发送整个数据帧。

9-14．为什么某站点在发送第一帧之前，若检测到信道空闲就在等待时间 DIFS 后立即发送出去，但在收到第一帧的确认后并打算发送下一帧时，就必须执行退避算法。

答：因为（1）在发送它的第一帧之前检测到信道处于忙状态；

（2）每一次的重传；

（3）每一次的成功发送后再要发送下一帧。

9-15．无线局域网的 MAC 帧为什么要使用四个地址字段？请用简单的例子说明地址 3 的作用。

答：地址 4 用于自组网络，前三个地址的内容取决于帧控制字段中的“到 DS”（到分配系统）和“从 DS”（从分配系统）这两个子字段的数值。这两个子字段各占 1 位，合起来共有 4 种组合，用于定义 802.11 帧中的几个地址字段的含义。

例如：站点 A 向 B 发送数据帧，但这个过程要分两步走。首先要由站点 A 把数据帧发送到接入点 AP1，然后再由 AP1 把数据帧发送到站点 B。当站点 A 把数据帧发送到 AP1 时，帧控制字段中的“到 DS=1”而“从 DS=0”。因此地址 1 是 AP1 的 MAC 地址（接收地址），地址 2 是 A 的 MAC 地址（源地址），地址 3 是 B 的 MAC 地址（目的地址）。当 AP1 把数据帧发送到站点 B 时，帧控制字段中的“到 DS=0”而“从 DS=1”。 因此地址 1 是 B 的 MAC 地址(目的地址），地址 2 是 AP1 的 MAC 地址（发送地址），地址 3 是 A 的 MAC 地址（源地址）。

9-16．试比较 IEEE 802.3 和 IEEE802.11 局域网，找出它们之间的主要区别？

答：IEEE 最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中，用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到 2Mbps。目前，3Com 等公司都有基于该标准的无线网卡。由于 802.11 在速率和传输距离上都不能满足人们的需要，因此，IEEE 小组又相继推出了 802.11b 和 802.11a 两个新标准。三者之间技术上的主要差别在于 MAC 子层和物理层。

IEEE802.3：描述物理层和数据链路层的 MAC 子层的实现方法,在多种物理媒体上以多种速率采用 CSMA/CD 访问方式，对于快速以太网该标准说明的实现方法有所扩展。早期的 IEEE 802.3 描述的物理媒体类型包括:10Base2、10Base5、10BaseF、10BaseT 和 10Broad36 等；快速以太网的物理媒体类型包括：100 BaseT、100BaseT4 和 100BaseX 等。

9-17．无线个人区域网 WPAN 的主要特点是？现在已经有了什么标准？

答：主要特点：一个人为中心，低功率、小范围、低速率和低价格。
标准：由 IEEE 的 802.15 工作组制定的标准[W-IEEE802.15]

9-18．无线城域网 WMAN 的主要特点是什么？现在已经有了什么标准？

答：特点：运用宽带无线接入技术,可以将数据、Internet 、话音、视频和多媒体应用传送到商业和家庭用户，能够提供高速数据无线传输乃至于实现移动多媒体宽带业务。
标准：一个是 2004 年 6 月通过的 802.16 的修订版本，即 802.16d(它的正式名字是 802.16-2004)；另一个是 2005 年通过的 802.16 的增强版本，即 802.16e.

第 10 章 下一代因特网

10-1 NGI 和 NGN 各表示什么意思？它们的主要区别是什么？

答：NGN（Next Generation Internet）:即下一代英特网；NGI（Next Generation Network）:即下一代电信网。

主要区别：如表一所示 ：

表 1　NGN 与 NGI 的主要区别

	NGN	NGI
开放接口	业务与应用层	网络层
对外的业务创新空间	相对较小	相对很大
收费的主要层次	业务/应用层	网络层
是否区分消费者和提供者	严格区分	不区分，二者对等
收费理念	基本业务收费 增值业务收费	基本业务不收费 增值业务收费
业务的可管理性	要求网络也是可管理的	不要求网络也是可管理的

由此可见，NGN 希望业务提供者可以为用户(信息消费者)提供更好的融和业务，而 NGI 则希望为广大用户(不区分信息提供者和信息消费者)提供一个更好的创新平台。互联网与传统电信网在目标、设计原理、业务与应用、技术、市场、驱动力等方面的差异巨大，因此应采用与传统电信网不同的技术、管理和政策手段来看待和处理互联网所面临的问题。

10-2 建议的 IPv6 协议没有首部检验和。这样做的优缺点是什么？

答：优点：对首部的处理更简单。数据链路层已经将有差错的帧丢弃了，因此网络层可省去这一步骤；缺点：可能遇到数据链路层检测不出来的差错。

10-3 在 IPv4 首部中有一个“协议”字段，但在 IPv6 的固定首部中确没有。这是为什么？

答：在 IP 数据报传送的路径上的所有路由器都不需要这一字段的信息。只有目的主机才需要协议字段。在 IPv6 使用“下一个首部”字段完成 IPv4 中的“协议”字段的功能。

10-4 当使用 IPv6 时，ARP 协议是否需要改变？如果需要改变，那么应当进行概念性的改变还是技术性的改变？

答：从概念上讲没有改变，但因 IPv6 地址长度增大了，所以相应的字段都需要增大。

10-5 IPv6 只允许在原点进行分片。这样做有什么好处？

答：分片与重装是非常耗时的操作.IPV6 把这一功能从路由器中删除,并移到网络边缘的主机中,就可以大大的加快网络中 IP 数据的转发速度.

10-6 设每隔 1 微微秒就分配出 100 万个 IPv6 地址。试计算大约要用多少年才能将 IPv6 地址空间全部用光。可以和宇宙的年龄（大约有 100 亿年）进行比较。

答：IPv6 的地址重建共有 2 的 128 次方个地址,或 3.4×10 的 38 次方.1 秒种分配 10 的 18 次方个地址,可分配 1.08×10 的 13 次方年.大约是宇宙年龄的 1000 倍.地址空间的利用不会是均匀的.但即使只利用那个整个地址空间的 1/1000,那也是不可能那个用完的.

10-7 试把以下的 IPv6 地址用零压缩方法写成简洁形式：

（1）0000:0000:F53:6382:AB00:67DB:BB27:7332

（2）0000:0000:0000:0000:0000:0000:004D:ABCD

（3）0000:0000:0000:AF36:7328:0000:87AA:0398

（4）2819:00AF:0000:0000:0000:0035:0CB2:B271

答：(1) ::F53:6382:AB00:67DB:BB27:7332　　(2)::4D:ABCD　　(3)::AF36:7328:0:87AA:398　　(4)2819:AF::35:CB2:B271

10-8 试把以下的 IPv6 地址用零压缩方法写成简洁形式：

（1）0::0 (2)0:AA::0 (3)0:1234:3 (4)123::1:2

答：(1)0000:0000:0000:0000:0000:0000:0000:0000

(2)0000:00AA:0000:0000:0000:0000:0000:0000

(3)0000:1234:0000:0000:0000:0000:0000:0003

(4)0123:0000:0000:0000:0000:0000:0001:0002

10-9 以下的每一个地址属于哪一种类型？（1）FE80::12 (2)FEC0::24A2 (3)FF02::0 (4)0::01

答：（1）本地链路单播地址 （2）IETF 保留 （3）多播地址 （4）环回地址

10-10 从 IPv4 过渡到 IPv6 的方法有哪些？

答：如何完成从 IPv4 到 IPv6 的转换是 IPv6 发展需要解决的第一个问题。现有的几乎每个网络及其连接设备都支持 IPv4，因此要想一夜间就完成从 IPv4 到 IPv6 的转换是不切实际的。IPv6 必须能够支持和处理 IPv4 体系的遗留问题。可以预见，IPv4 向 IPv6 的过渡需要相当长的时间才能完成。目前，IETF 已经成立了专门的工作组，研究 IPv4 到 IPv6 的转换问题，并且已提出了很多方案，主要包括以下几个类型：

1. 双协议栈技术

IPv6 和 IPv4 是功能相近的网络层协议，两者都基于相同的物理平台，而且加载于其上的传输层协议 TCP 和 UDP 又没有任何区别。由图 1 所示的协议栈结构可以看出，如果一台主机同时支持 IPv6 和 IPv4 两种协议，那么该主机既能与支持 IPv4 协议的主机通信，又能与支持 IPv6 协议的主机通信，这就是双协议栈技术的工作机理。

图 1 IPv4/v6 双协议栈的协议结构

图 2 示出了通过双协议栈的通信方式，图中的双协议主机可以分别和 IPv6 主机及 IPv4 主机互通。

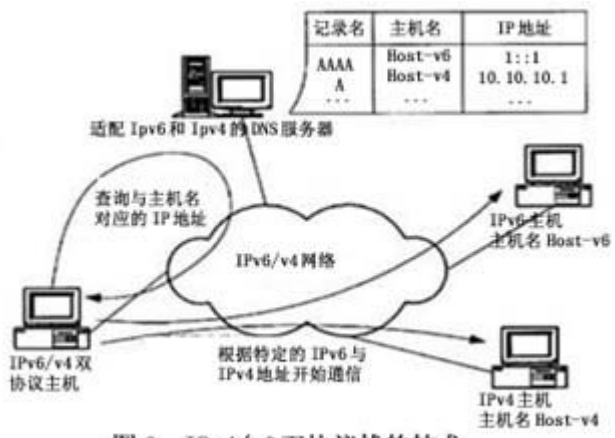


图 2　IPv4/v6 双协议栈的技术

2. 隧道技术

随着 IPv6 网络的发展，出现了许多局部的 IPv6 网络，但是这些 IPv6 网络需要通过 IPv4 骨干网络相连。将这些孤立的“IPv6 岛”相互联通必须使用隧道技术。利用隧道技术可以通过现有的运行 IPv4 协议的 Internet 骨干网络（即隧道）将局部的 IPv6 网络连接起来，因而是 IPv4 向 IPv6 过渡的初期最易于采用的技术。

路由器将 IPv6 的数据分组封装入 IPv4，IPv4 分组的源地址和目的地址分别是隧道入口和出口的 IPv4 地址。在隧道的出口处，再将 IPv6 分组取出转发给目的站点。隧道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，因而非常容易实现。但是隧道技术不能实现 IPv4 主机与 IPv6 主机的直接通信。

3. 网络地址转换/协议转换技术

网络地址转换/协议转换技术 NAT-PT(Network Address Translation - Protocol Translation)通过与 SIIT 协议转换和传统的 IPv4 下的动态地址翻译（NAT）以及适当的应用层网关（ALG）相结合，实现了只安装了 IPv6 的主机和只安装了 IPv4 机器的大部分应用的相互通信。

10-11 多协议标记交换 MPLS 的工作原理是怎样的？它有哪些主要的功能？

答：MPLS 的工作原理 ：MPLS 是基于标记的 IP 路由选择方法。这些标记可以被用来代表逐跳式或者显式路由，并指明服务质量（QoS）、虚拟专网以及影响一种特定类型的流量（或一个特殊用户的流量）在网络上的传输方式等各类信息。MPLS 采用简化了的技术，来完成第三层和第二层的转换。它可以提供每个 IP 数据包一个标记，将之与 IP 数据包封装于新的 MPLS 数据包，由此决定 IP 数据包的传输路径以及优先顺序，而与 MPLS 兼容的路由器会在将 IP 数据包按相应路径转发之前仅读取该 MPLS 数据包的包头标记，无须再去读取每个 IP 数据包中的 IP 地址位等信息，因此数据包的交换转发速度大大加快。

目前的路由协议都是在一个指定源和目的地之间选择最短路径，而不论该路径的带宽、载荷等链路状态，对于缺乏安全保障的链路也没有一种显式方法来绕过它。利用显式路由选择，就可以灵活选择一条低延迟、安全的路径来传输数据。

MPLS 协议实现了第三层的路由到第二层的交换的转换。MPLS 可以使用各种第二层协议。MPLS 工作组到目前为止已经把在帧中继、ATM 和 PPP 链路以及 IEEE802．3 局域网上使用的标记实现了标准化。MPLS 在帧中继和 ATM 上运行的一个好处是它为这些面向连接的技术带来了 IP 的任意连通性。目前 MPLS 的主要发展方向是在 ATM 方面。这主要是因为 ATM 具有很强的流量管理功能，能提供 QoS 方面的服务，ATM 和 MPLS 技术的结合能充分发挥在流量管理和 QoS 方面的作用。标记是用于转发数据包的报头，报头的格式则取决于网络特性。在路由器网络中，标记是单独的 32 位报头；在 ATM 中，标记置于虚电

路标识符 / 虚通道标识符（VCI / VPI）信元报头中。对于 MPLS 可扩展性非常关键的一点是标记只在通信的两个设备之间有意义。在网络核心，路由器 / 交换机只解读标记并不去解析 IP 数据包。　　IP 包进入网络核心时，边界路由器给它分配一个标记。自此，MPLS 设备就会自始至终查看这些标记信息，将这些有标记的包交换至其目的地。由于路由处理减少，网络的等待时间也就随之缩短，而可伸缩性却有所增加。MPLS 数据包的服务质量类型可以由 MPLS 边界路由器根据 IP 包的各种参数来确定，如 IP 的源地址、目的地址、端口号、TOS 值等参数。

对于到达同一目的地的 IP 包，可根据其 TOS 值的要求来建立不同的转发路径，以达到其对传输质量的要求。同时，通过对特殊路由的管理，还能有效地解决网络中的负载均衡和拥塞问题。当网络中出现拥塞时，MPLS 可实时建立新的转发路由来分散流量以缓解网络拥塞。

10-12 试讨论在 MPLS 域中的三种流的聚合程度：（1）所有的 IP 数据报都是流向同一个主机；（2）所有的 IP 数据报都流经同一个出口 LSR；（3）所有的 IP 数据报都具有同样的 CIDR 地址。

答：（1）聚合粒度细；（2）聚合力度稍微粗些 ，出口 LSR 要检查每个分组的首部，以便将其分配到合适的终点；（3）这是最粗的聚合粒度，许多网络中的流都将聚合为同一个流，而这种聚合路径通常都在 MPLS 的主干网中。

10-13 什么叫显示路由选择？它和通常在因特网中使用的路由选择有何区别？

答：显式路由选择:该方案基于由交换路由器或 ATM 交换机组成的网络。显式路由使用流量工程技术或者手工制定路由，不受动态路由影响，路由计算中可以考虑各种约束条件（如策略、CoS 等级），每个 LSR 不能独立地选择下一跳，而由 LSP 的入口/出口 LSR 规定位于 LSP 上的 LSR。提前为数据分组指明预定义路径。这是在 ATM 世界中的虚拟线路。由于预定义了路径,数据分组在每一节点交换,因此不再需要在沿途每一节点上做出路由选择决定。对于通信工程、QoS（服务质量)和防止路由选择循环,显示路由选择很有用。它要求提前建立路径,有些可在 IP 网络中用 MPLS(多协议标签交换)完成。源路由选择是显示路由选择的一种形式,它是在发送数据分组之前,端系统发现通过网络的路径。

10-14 MPLS 能否使用显示路由选择以保证对特定流的 QoS 需求？请说明理由

答：可以。但有关这种 QoS 需求的信息应当使边沿路由器知道。

10-15 试给出两个例子分别在细粒度和粗力度上使用 QoS 显式路由选择

答：细粒度：按照源点和终点间的每一个应用流定义 QoS 需求。

粗粒度：按照一组网络前缀或两个网络之间的应用流定义 QoS 需求。

10-16 试比较网络在以下三种情况的可扩展性：

（1）仅使用第三层转发：每一个路由器查找最长前缀匹配以确定下一跳；

（2）第三层转发和第二层 MPLS 转发；

（3）仅有第二层 MPLS 转发

答：（1）当路由表很大时查找最长前缀匹配需要很长时间，这就限制了网络的规模 （2）若有许多的分组使用 MPLS 就可缩短转发分组所需的时间，因而网络可扩展到极大的规模；（3）分组经受的时候最小，分组转发的速率不受路由表大小的影响。但网络节点无法处理没有 MPLS 标记的分组。

10-17 在 Diffserv 中的边界结点和 MPLS 中的入口结点是否都是同样性质的结点？Diffserv 中的边界路由器和 MPLS 入口的结点的标记交换路由器一样吗？

答：两者有相似处，但具体功能不同。具体功能如下：

Diffserv 将所有的复杂性放在 DS 域的边界结点中，而使 DS 域内部路由器工作的尽可能的简单。边界结点可以是主机，路由器，或防火墙等。其中边界路由器中的功能很多，可分为分类器和通信量调节器两大部分。调节器又由标记器，整形器和侦测器 3 个部分组成。

LSR（即标记交换路由器）同时具有标记交换和路由选择这两个功能，标记转换功能是为了快速转发，但在这之前 LSR 需要使用路由选择功能构造转发表。当一个 IP 数据报进入到 MPLS 域时，MPLS 入口结点就给它打上标记，并按照转发表把他转发给下一个 LSR。以后的所有 LSR 都按照标记进行转发。由于再全网内统一分配全局标记数值是非常困难的，因此一个标记仅仅在两个标记路由器 LSR 之间才有意义。

10-18 在防火墙中的分组过滤和 MPLS 标记交换是否兼容？请说明理由。

答：防火墙中的分组过滤工作在 IP 或者 IP 层以上，而 MPLS 标记交换则工作在 IP 层以下。分组过滤就是从分

组首部提取出特定的字段，然后暗战事先制定好的规则对分组进行处理。防火墙本来不处理 IP 层以下的 MPLS 的首部。但现在的网络处理机的功能增强了，可以从一个分组的多个首部中提取和处理多个字段的功能。因此，MPLS 可以建立这样的显式路径，其出口结点有防火墙。

10-19 现在流行的 P2P 文件共享应用程序都有哪些特点？存在哪些值得注意的问题？

答：这种工作方式不需要使用集中式的媒体服务器，这就解决了集中式媒体服务器可能出现的瓶颈问题。

在 P2P 工作方式下，所有的音频/视频文件都是在普通的因特网用户之间传输。这其实是相当于有很多（有时达到上百万个）分散在各地的媒体服务器（由普通用户的 PC 机充当这种服务器）其他用户提供所要下载的音频/视频文件。

随着 P2P 文件共享程序日益广泛地使用也产生了一系列的问题有待于解决。如，音频/视频文件的知识产权就是其中的一个问题。又如，当非法盗版的，或不健康的音频/视频在因特网上利用 P2P 文件共享程序广泛传播时,要对 P2P 的流量进行有效的管理，在技术上还是又相当的难度。由于现在 P2P 文件共享程序的大量使用，已经消耗了因特网主干网上大部分的宽带，但网络经营商并没有因此而盈利。因此，怎样制定出合理的收费标准，既能够让广大网民接受，又能让网络经营商有利可图，也是目前迫切需要解决的问题。