# 习题解答

习题及参考答案说明

习题中的某些问答题是为了方便学生课后理解书本知识，并不一定适合作为考试题目，给出的答案也仅供参考，学生不应该死记硬背。

## 第1章

1-1 计算机网络向用户可以提供哪些服务？

解答：计算机网络是一种通信基础设施，向用户提供的最核心的服务就是信息交互服务和资源共享服务。虽然计算机网络与电信网络和有线电视网络一样，都是一种通信基础设施，但与这两个网络最大的不同在于计算机网络的端设备是功能强大且具有智能的计算机。利用计算机网络这个通信基础设施，计算机上运行的各种应用程序通过彼此间的通信能为用户提供更加丰富多彩的服务和应用，如文件传输、电子邮件、网络电视等待。

1-2 试简述分组交换的要点。

解答：分组交换采用存储转发技术，当需要发送数据时无需在源和目的之间先建立一条物理的通路，而是将要发送的报文分割为较小的数据段，将控制信息作为首部加在每个数据段前面（构成分组）一起发送给分组交换机。每一个分组的首部都含有目的地址等控制信息。分组交换网中的分组交换机根据分组首部中的控制信息，把分组转发到下一个分组交换机。用这种存储转发方式将分组转发到达最终目的地。

1-3 试从建立连接、何时需要地址、是否独占链路、网络拥塞、数据是否会失序、端到端时延的确定性、适用的数据传输类型等多个方面比较分组交换与电路交换的特点。

解答：

| 电路交换 | 分组交换 |
| --- | --- |
| 通信前需要建立连接 | 通信前可以不建立连接 |
| 通信过程中始终占用端到端的固定传输带宽 | 分组在链路上传输时仅逐段占用经过的链路 |
| 通信时线路上不会因为拥塞而丢失数据 | 通信时会因为网络拥塞而导致分组丢失 |
| 数据按序到达 | 分组可能失序 |
| 建立连接后通信过程中不再需要地址 | 所有分组都携带地址或相关控制信息 |

| | |
|---|---|
| 端到端时延确定 | 端到端时延不确定 |
| 适合大量实时数据的传输 | 适合突发数据的传输 |

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？

解答：因特网已成为仅次于全球电话网的世界第二大网络，缩小了人际交往的时间和空间，大大改变着我们工作和生活的各个方面。

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。

解答：因特网的基础结构大体上经历了三个阶段的演进。第一阶段——从单个网络 ARPANET 向互联网发展。第二阶段——逐步建成了三级结构的因特网。第三阶段——逐渐形成了多层次 ISP 结构的因特网。

1-6 试简述因特网标准制定的几个阶段。

解答：制订因特网的正式标准要经过以下的四个阶段：

（1）因特网草案（Internet Draft）——在这个阶段还不是 RFC 文档。

（2）建议标准（Proposed Standard）——从这个阶段开始就成为 RFC 文档。

（3）草案标准（Draft Standard）。

（4）因特网标准（Internet Standard）。

1-7 小写和大写开头的英文名字 internet 和 Internet 在意思上有何重要区别？

解答：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连而成的网络。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）则是一个专用名词，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，且其前身是美国的 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？

解答：见 1.4.2 节。

1-9 因特网的两大组成部分（边缘部分与核心部分）的特点是什么？它们的工作方式各有什么特点？

解答：因特网的拓扑结构虽然非常复杂，并且在地理上覆盖了全球，但从其工作方式上看，可以划分为以下的两大块：

（1）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。

（2）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）。

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)。从源点到终点共经过 $k$ 段链路，每段链路的传播时延为 $d$ (s)，数据传输速率为 $b$ (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)，假设 x > p 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？（提示：画一下草图观察 $k$ 段链路共有几个结点。）

解答：分组交换时延为：$(k-1)p/b+k\cdot d+x/b$。电路交换时延为：$s+k\cdot d+x/b$。因此，

分组交换时延较电路交换时延小的条件为：$(k-1)p/b<s$

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。链路的数据传输速率为 $b$ (bit/s)，结点的排队时间可忽略不。若打算使总的时延为最小，问分组的数据部分长度 $p$ 应取多大？

解答：假设每段链路的传播时延为 $d$ (s)，计算总时延 $D$ 为：

$(k-1)(p+h)/b+k\cdot d+x/b+(x/p)h/b$,

求 $D$ 对 $p$ 的导数，令其为零。解出

$$p=\sqrt{xh/(k-1)}$$

1-12 从差错控制、时延和资源共享 3 个方面分析，分组交换为什么要将长的报文划分为多个短的分组进行传输？

答：（1）若报文太大在传输中出现差错的概率大，并且一旦出现差错可能要重传整个报文，而划分为小的分组，该分组出现差错的概率减小了，并且一次仅需要重传一个分组。（2）将长的报文划分为多个短的分组可以减小储存转发的时延。（3）太大的报文占用链路太长，不利于资源共享，将长的报文划分为多个短的分组减小的资源共享的粒度，提高整个系统的平均响应时间，例如如一台计算机在传输大的文件时，而另一台计算机通过同一链路可以上网浏览网页，而无需等待文件传输结束。

1-13 计算机网络有哪些常用的性能指标？

解答：速率、带宽、吞吐量、时延、利用率

1-14 收发两端之间的传输距离为 1000 km，信号在媒体上的传播速率为 $2\times10^8$ m/s。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 $10^7$ bit，数据发送速率为 100 kbit/s；

（2）数据长度为 $10^3$ bit，数据发送速率为 1 Gbit/s。

从以上计算结果可得出什么结论？

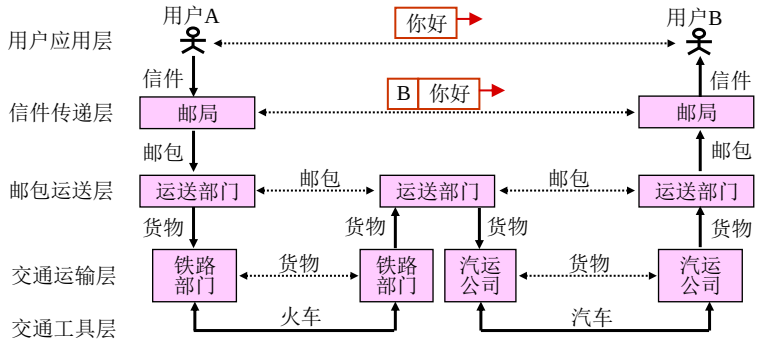
解答：(1) 发送时延为 100 s，传播时延为 5 ms。发送时延远大于传播时延。

(2) 发送时延为 1 μs，传播时延为 5 ms。发送时延远小于传播时延。

1-15 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中的例子。

解答：网络体系结构采用分层结构是因为“分层”可将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题就比较易于研究和处理。

在我们的日常生活中不乏层次结构的系统，例如邮政系统就是一个分层的系统，而且它与计算机网络有很多相似之处，如图所示。




1-16 协议与服务有何区别？有何关系？

解答：这些为进行网络中的数据交换而建立的规则或约定称为网络协议（network protocol）。网络协议也可简称为协议。协议是控制两个对等实体（或多个实体）进行通信的规则的集合。在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。要实现本层协议，还需要使用下面一层所提供的服务。

协议和服务在概念上是很不一样的。首先，协议的实现保证了能够向上一层提供服务。使用本层服务的实体只能看见服务而无法看见下面的协议。其次，协议是“水平的”，即协议是控制对等实体之间通信的规则。但服务是“垂直的”，即服务是由下层向上层通过层间接口提供的。另外，并非在一个层内完成的全部功能都称为服务。只有那些能够被高一层实体“看得见”的功能才能称之为“服务”。

1-17 试述具有五层协议的网络体系结构的要点，包括各层的主要功能。

解答：

(1) 物理层：在物理媒体上传送比特流。具体包括：与物理媒体的接口、比特的表示与同步、数据率、线路配置、物理拓扑等。

(2) 数据链路层：在两个相邻结点间（主机和路由器或路由器和路由器之间）的链路上传送以帧为单位的数据。具体包括：组帧、差错控制、物理编址、接入控制、流量控制等。

(3) 网络层：负责将分组从源主机（按照合适的路由）通过中间若干路由器的转发传送到目的主机。核心功能是逻辑编址、路由选择和分组转发。

(4) 运输层：负责主机中两个进程之间的逻辑通信（端到端通信）。具体包括：复用与分用、可靠数据传输、流量控制、拥塞控制等。

(5) 应用层：通过应用进程间的交互来实现特定网络应用，直接为用户或应用进程提供特定的应用服务，如文件传输、电子邮件等。

1-18 试解释以下名词：协议栈、实体、对等层、协议数据单元、客户、服务器、客户–服务器方式。

解答：

协议栈：将网络协议几个层次画在一起很像一个栈的结构，因此将这些协议层称为协议栈。

实体：表示任何可发送或接收信息的硬件或软件进程。

对等层：通信双方实现同样功能的层。协议定义的就是对等层间的通信规则。

协议数据单元：OSI 参考模型把对等层次之间传送的数据单位称为该层的协议数据单元 PDU。

客户：在计算机网络中进行通信的应用进程中的服务请求方。

服务器：在计算机网络中进行通信的应用进程中的服务提供方。

客户–服务器方式：通常指的是一种网络应用程序的工作方式。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。客户是服务请求方，服务器是服务提供方。服务器总是一直运行并被动等待通信，而客户总是主动发起通信。服务器可以同时处理多个客户的请求，而客户程序之间不直接进行通信。

1-19 试解释 everything over IP 和 IP over everything 的含义。

解答：TCP/IP 协议可以为各式各样的应用提供服务，即 IP 协议之上可以运行各种各样的网络应用，这就是所谓的 everything over IP。同时 TCP/IP 协议也允许 IP 协议互连各种各式各样的物理网络而构成的互联网，在 IP 层以上看不见下层不同的物理网络，这就是所谓的 IP over everything。

1-20 判断以下正误。

（1）提高链路速率意味着降低了信道的传播时延。（×）

原因：

提高链路速率是提高了将数据推送到链路的速率。而信道的传播时延仅跟信号的传播速率和信道长度有关，与发送速率无关。因此提高链路速率不会影响信道的传播时延。

（2）在链路上产生的传播时延与链路的带宽无关。（√）

原因：

由于承载信息的电磁波在通信线路上的传播速率（这是光速的数量级）与数据的发送速率并无关系，因此在链路上产生的传播时延仅与信号传播速率和信道长度有关。

（3）跨越网络提供主机到主机的数据通信的问题属于运输层的功能。（×）

原因：

跨越网络提供主机到主机的数据通信的问题属于网络层的功能。运输层为不同主机上的

应用进程和应用进程间提供逻辑通信功能。

（4）发送时延是分组的第一个比特从发送方发出到该比特到达接收方之间的时间。（×）

原因：

发送时延是主机或路由器将分组发送到通信线路上所需要的时间，也就是从发送分组的第一个比特算起，到该分组的最后一个比特发送到线路上所需要的时间。

（5）由于动态分配通信带宽和其他通信资源，分组交换能更好更高效地共享资源。（√）

（6）采用分组交换在发送数据前可以不必先建立连接，发送突发数据更迅速，因此不会出现网络拥塞。（×）

原因：

由于分组交换不像电路交换那样通过建立连接来保证通信时所需的各种资源，因而无法确保通信时端到端所需的带宽，在通信量较大时可能造成网络拥塞。

1-21 一个系统的协议结构有 N 层，应用程序产生 M 字节长的报文，网络软件在每层都加上 h 字节的协议头，网络带宽中至少有多大比率用于协议头信息的传输？

解答：$(N \times h/(N \times h + M)) \times 100\%$。若应用程序产生的报文再分为多个小的分组则比率会更大。

## 第 2 章

2-1 物理层要解决哪些问题？物理层协议的主要任务是什么？

解答：物理层考虑的是怎样才能在连接各种计算机的传输媒体上传输数据比特流，而不是指具体的传输媒体。因此物理层要考虑如何用电磁信号表示“1”或“0”；考虑所采用的传输媒体的类型，如双绞线、同轴电缆、光缆等；考虑与物理媒体之间接口，如插头的引脚数目和排列等；考虑每秒发送的比特数目，即数据率。

物理层协议的主要任务就是确定与传输媒体的接口有关的一些特性，即机械特性、电气特性、功能特性和过程特性。

2-2 规程与协议有什么区别？

解答：用于物理层的协议也常称为物理层**规程**（procedure）。其实物理层规程就是物理层协议。只是在“协议”这个名词出现之前人们就先使用了“规程”这一名词。

2-3 物理层的接口有哪几个方面的特性？各包含些什么内容？

解答：

（1）机械特性 指明接口所用接线器的形状和尺寸、引脚数目和排列、固定和锁定装置等。常见的各种规格的电源接插件都有严格的标准化的规定。

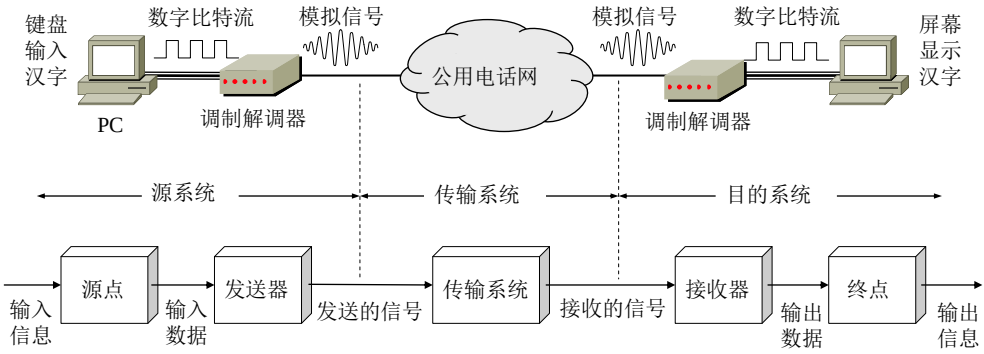
（2）电气特性 指明在接口电缆的各条线上出现的电压的范围。

（3）功能特性 指明某条线上出现的某一电平的电压表示何种意义。

（4）过程特性 指明对于不同功能的各种可能事件的出现顺序。

2-4 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。

解答：一个数据通信系统可划分为三大部分，即源系统（或发送端、发送方）、传输系统（或传输网络）和目的系统（或接收端、接收方）。




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，从 PC 的键盘输入汉字，PC 产生输出的数字比特流。源点又称为源站或信源。

发送器：通常源点生成的数字比特流要通过发送器编码后才能够在传输系统中进行传输。典型的发送器就是调制器。现在很多 PC 使用内置的调制解调器（包含调制器和解调器），用户在 PC 外面看不见调制解调器。

目的系统一般也包括以下两个部分：

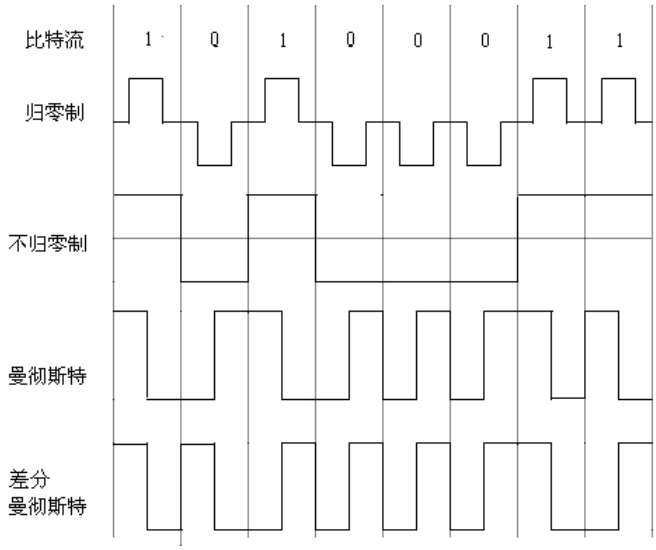
接收器：接收传输系统传送过来的信号，并把它转换为能够被目的设备处理的信息。典型的接收器就是解调器，它把来自传输线路上的模拟信号进行解调，提取出在发送端置入的消息，还原出发送端产生的数字比特流。

终点：终点设备从接收器获取传送来的数字比特流，然后进行信息输出（例如，把汉字在 PC 屏幕上显示出来）。终点又称为目的站或信宿。

在源系统和目的系统之间的传输系统可以是简单的传输线，也可以是连接在源系统和目的系统之间的复杂网络系统。

2-5　请画出数据流 1 0 1 0 0 0 1 1 的不归零编码、曼彻斯特编码和差分曼彻斯特编码的波形（从高电平开始）。

解答：所求波形图如图所示。




题 2-5 之图

2-6 “比特/秒”和“码元/秒”有何区别？

解答：“比特/秒”和“码元/秒”是不完全一样的，信息的传输速率“比特/秒”与码元的传输速率“波特”（“码元/秒”）在数量上却有一定的关系。若 1 个码元只携带 1 bit 的信息量，则“比特/秒”和“波特”在数值上是相等的。但若使 1 个码元携带 $n$ bit 的信息量，则 $M$ Baud 的码元传输速率所对应的信息传输速率为 $M \times n$ bit/s。

2-7 假定某信道受奈氏准则限制的最高码元速率为 20000 码元/秒。如果采用幅移键控，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）？

解答：16 个等级可以表达 4 位二进制数，每个码元可以表示 4 个比特，因此，可以获得 80000 b/s 的数据率。

2-8 假定用 3 kHz 带宽的电话信道传送 64 kb/s 的数据，试问这个信道应具有多高的信噪比？

解答：根据香农公式：$C = 3 \times \log_2(1 + S/N) = 64$，$1 + S/N = 2^{64/3}$

$S/N \approx 2.64 \times 10^6$

2-9 试解释以下名词：数据，信号，模拟信号，基带信号，带通信号，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。

解答：

数据：运送消息的实体。

信号：数据的电气或电磁表现。

模拟信号：连续信号，其特点是其代表消息的信号参数的取值是连续变化的。

基带信号：来自信源的信号（没有经过调制和搬移过频谱的信号），因为往往包含有较多的低频成分，甚至有直流成分，因此常被称为基带信号（即基本频带信号）。

带通信号：经过载波调制后的信号（把基带信号的频率范围搬移到较高的频段以便在信道中传输）称为带通信号（即仅在一段频率范围内能够通过信道）。

数字信号：离散信号，代表消息的信号参数的取值是离散的。

码元：在使用时间域（或简称为时域）的波形表示数字信号时，代表不同离散数值的基本波形就称为码元。码元是承载信息的基本信号单位。

单工通信：即只能有一个方向的通信而没有反方向的交互。

半双工通信：即通信的双方都可以发送信息，但不能双方同时发送（当然也就不能同时接收）。这种通信方式是一方发送另一方接收，过一段时间后再反过来。

全双工通信：即通信的双方可以同时发送和接收信息。

串行传输：数据在传输时是逐个比特按照时间顺序依次传输。

并行传输：数据在传输时采用 n 个并行的信道，一次同时传输 n 个比特。

2-10 常用的传输媒体有哪几种？各有何特点？

解答：

双绞线，用两根绝缘铜线扭在一起的通信媒体，绞合在一起是为了减少相邻导线的电磁干扰。双绞线可分为屏蔽双绞线和非屏蔽双绞线。在数字传输时，若传输速率为每秒几个兆比特，则传输距离可达几公里。双绞线价格便宜，布线方便，主要用于电话用户线和局域网中。

同轴电缆，由内导体铜质芯线、绝缘层、网状编织的外导体屏蔽层以及保护塑料外层所组成。同轴电缆的这种结构和屏蔽性使得它有比双绞线高得多的带宽和更好的抗干扰特性。目前同轴电缆主要用在有线电视网的居民小区中。

光纤，是利用光导纤维传递光脉冲信号来进行通信，由于可见光的频率非常高（108MHz），因此一个光纤通信系统的传输带宽远远大于目前其他传输媒体的带宽。光纤可分为单模光纤和多模光纤。光纤不仅通信容量非常大，而且传输损耗小，抗干扰和保密性能好。光纤通常用在主干网络中和高速局域网中。

无线传输媒体，即利用自由空间传播电磁波。当通信距离很远，或跨越复杂地理环境时，铺设电缆既昂贵又费时，利用无线电波在自由空间传播，可以实现多种通信。无线传输所使用的频段很广。人们现在利用无线电、微波、红外线以及可见光这几个波段进行通信。无线传输媒体的最大缺点就是容易被干扰，保密性差。

2-11 为什么要使用信道复用技术？常用的信道复用技术有哪些？

解答：许多用户可以通过复用技术共同使用一个共享的信道来进行通信。当网络中传输媒体的传输容量大于单一信道传输的通信量时，可利用复用技术在一条物理线路上建立多条通信信道来充分利用传输媒体的带宽。

常用的复用技术包括：频分复用、时分复用、波分复用、码分复用。

2-12 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

解答：

FDM(Frequency Division Multiplexing)频分复用，将传输线路的可用频带分割为若干条较窄的子频带，每一条子频带传输一路信号，从而实现在同一条线路上传输多路信号。

TDM(Time Division Multiplexing)时分复用，将一条物理线路的传输时间分成若干个时间片（时隙），按一定的次序轮流给各个信号源使用，从而实现在同一条线路上传输多路信号。

STDM(Statistic TDM)统计时分复用，又称为异步时分复用，将线路的传输时间按需动态地分配给各个信号源，而不是给每个信号源分配固定的时隙。

WDM(Wavelength Division Multiplexing)波分复用，就是光的频分复用，将不同波长的光信号复用到同一根光纤上。

DWDM(Dense WDM)密集波分复用，最初，人们只能在一根光纤上复用两路光载波信号。这种复用方式称为波分复用 WDM。随着技术的发展，在一根光纤上复用的光载波信号的路数越来越多。现在已能做到在一根光纤上复用几十路或更多路数的光载波信号。于是就使用了密集波分复用 DWDM 这一名词。DWDM 的波长间隔很小，不到 2 nm。

CDMA(Code Division Multiplex Access)码分多址，给每个用户分配一个唯一的正交码，在发送端，不同用户的数据用该正交码编码后复用到同一信道进行传输；在接收端，用同一正交码解码进行分用。CDMA 主要用于无线通信，具有很强的抗干扰能力。

SONET(Synchronous Optical Network)同步光纤网，美国在 1988 年首先推出的一个在光纤传输基础上的数字传输标准。整个同步网络的各级时钟都来自一个非常精确的主时钟。SONET 为光纤传输系统定义了同步传输的线路速率等级结构，其传输速率以 51.84 Mbit/s 为基础。

SDH(Synchronous Digital Hierarchy)同步数字系列，ITU-T 以美国标准 SONET 为基础制定的国际标准，SDH 的基本速率为 155.52 Mbit/s。

STM-1(Synchronous Transfer Module-1)第 1 级同步传递模块，是 SDH 的一系列传输标准之一，规定了 SDH 的基本速率为 155.52 Mbit/s。

OC-48(Optical Carrier-48) 第 48 级光载波，是 SONET 的一系列传输标准之一，其速率是 SONET 第 1 级光载波 OC-1 速率（51.84 Mbit/s）的 48 倍，即 2488.32 Mbit/s。

2-13 码分多址 CDMA 的复用方法有何优缺点？

解答：优点是容量大，有很强的抗干扰能力，发送功率小。缺点是技术相对复杂。

2-14 共有 4 个用户进行 CDMA 通信。这 4 个用户的码片序列为：

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)

现收到码片序列：(–1 +1 –3 +1 –1 –3 +1 +1)。问是哪些用户发送了数据？发送的是 1 还是 0？

解答：A 的内积为 1，B 的内积为–1，C 的内积为 0，D 的内积为 1。因此，A 和 D 发送的是 1，B 发送的是 0，而 C 未发送数据。

2-15 试比较 ADSL、HFC 及 FTTx 接入技术的特点。

解答：ADSL 最大好处是利用现有电话网中的用户线，改造成本低，每户独占该用户线，并可以同时上网和打电话，但接入速率与用户线的质量和长度有很大关系。

HFC 的优点是利用现有的有线电视系统，传输带宽高，但要将现有单向传输的有线电视电缆改造为双向通信的电缆，小区用户共享同一媒体。

FTTx 带宽高，是解决宽带接入最理想的方案，但需要铺设大量光纤，投入的建设成本较高。

2-16 为什么在 ADSL 技术中，在不到 1 MHz 的带宽中可以传送的速率却可以高达每秒几个兆比特？

解答：采用先进的编码技术，每个码元携带多个比特，即每秒传送一个码元就相当于每秒传送多个比特。

2-17 判断以下正误。

（1）DSL 和电话网拨号接入技术都要通过电话网经过电话交换机连接到 ISP 的路由器的。（×）

原因：拨号上网使用拨号调制解调器，利用电话网（电路交换）在用户计算机与 ISP 的路由器之间建立一条物理链路（话音信道），使用这条话音信道传输数据。而 DSL 仅使用用户线，利用频分复用技术将用户线划分了数据信道和话音信道分离，上网的数据并不通过电话网。

（2）通过 ADSL 上网的同时可以利用同一电话线打电话。（√）

原因：ADSL 仅使用用户线，利用频分复用技术将用户线划分了数据信道和话音信道分离，上网的数据并不通过电话网，因此可以同时上网和打电话。

（3）双绞线由两个具有绝缘保护层的铜导线按一定密度互相绞在一起组成，这样不容易被拉断。（×）

原因：双绞线由两个具有绝缘保护层的铜导线按一定密度互相绞在一起组成，这样可以降低信号干扰的程度。

（4）信道复用技术可以将多路信号复用到同一条传输线路上进行传输，而不会混淆，因此能将该传输线路的带宽成倍增加。（×）

2-18 请比较电话网拨号上网和通过 ADSL 上网的区别。

解答：拨号上网使用拨号调制解调器，利用电话网（电路交换）在用户计算机与 ISP 的路由器之间建立一条物理链路（话音信道），使用这条话音信道传输数据，因此不能同时打电话和上网。而 ADSL 仅使用用户线，利用频分复用技术将用户线划分了数据信道和话音信道分离，上网的数据并不通过电话网，因此可以同时上网和打电话，并且因为不受话音信道频带宽度的限制可以提供更高的数据带宽。

## 第 3 章

3-1 数据链路（即逻辑链路）与链路（即物理链路）有何区别？“电路接通了”与“数据链路接通了”的区别何在？

解答：所谓链路就是从一个结点到相邻结点的一段物理线路，而中间没有任何其他的交换结点。在进行数据通信时，两个计算机之间的通信路径往往要经过许多段这样的链路。可见链路只是一条路径的组成部分。

数据链路则是另一个概念。这是因为当需要在一条线路上传送数据时，除了必须有一条物理线路外，还必须有一些必要的通信协议来控制这些数据的传输（这将在后面几节讨论）。若把实现这些协议的硬件和软件加到链路上，就构成了数据链路。这样的数据链路就不再是简单的物理链路而是个逻辑链路了。

“电路接通了”仅仅是物理线路接通了通信双方可以在上面发送和接收 0/1 比特了，而“数据链路接通了”表明在该物理线路接通的基础上通信双方的数据链路层协议实体已达成了一致并做好了在该链路上发送和接收数据帧的准备（可能互相要协商某些数据链路层参数）。

3-2 数据链路层包括哪些主要功能？试讨论数据链路层做成可靠的链路层有哪些优点和缺点。

解答：数据链路层的链路控制的主要功能包括：封装成帧、透明传输和差错检测，可选功能包括可靠传输、流量控制等。

在数据链路层实现可靠传输的优点是通过点到点的差错检测和重传能及时纠正相邻结点间传输数据的差错。若在数据链路层不实现可靠传输由高层如运输层通过端到端的差错检测和重传来纠正这些差错会产生很大的重传时延。

但是在数据链路层实现可靠传输并不能保证端到端数据传输的可靠，如由于网络拥塞导致路由器丢弃分组等。因此，即使数据链路层是可靠的，在高层如运输层仍然有必要实现端到端可靠传输。如果相邻结点间传输数据的差错率非常低，则在数据链路层重复实现可靠传输就会给各结点增加过多不必要的负担。

3-3 网络适配器的作用是什么？网络适配器工作在哪一层？

解答：网络适配器的作用就是实现数据链路层和物理层的功能。适配器接收和发送各种帧时不使用计算机的 CPU。这时 CPU 可以处理其他任务。当适配器收到有差错的帧时，就把这个帧丢弃而不必通知计算机。当适配器收到正确的帧时，它就使用中断来通知该计算机并交付给协议栈中的网络层。网络适配器工作在物理层和数据链路层。

3-4 如果不解决透明传输问题会出现什么问题？

解答：如果不解决透明传输问题，如果传输的数据中有与帧定界符相同的比特组合，则会导致帧定界错误。

3-5 要发送的数据为 1101011011。采用 CRC 的生成多项式是 $P(X)=X^4+X+1$。试求应添加在数据后面的余数。

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？

采用 CRC 检验后，数据链路层的传输是否就变成了可靠的传输？

解答：根据 CRC 生成多项式，除数 P=10011。用 11010110110000，模 2 除 P，余数即

CRC 检验序列为 1110。

添加检验序列后为 11010110111110，数据（注意是数据，不包括检验序列）在传输过程中最后一个 1 变成了 0，则接收方收到的数据为 11010110101110。除 P 得到的余数不为零（0011），发现差错。

若数据在传输过程中最后两个 1 都变成了 0，则接收方收到的数据为 11010110001110。除 P 得到的余数也不为零（0101），发现差错。

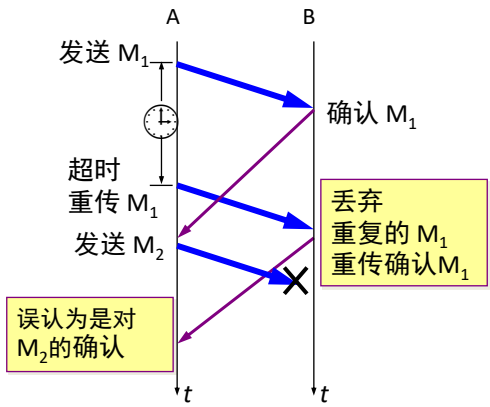
采用 CRC 检验仅能发现数据在传输过程中出现差错但并不能纠正差错，因此并不能实现可靠传输。

3-6 要发送的数据为 101110。采用 CRC 的生成多项式是 $P(X)=X^3+1$。试求应添加在数据后面的余数。

解答：根据 CRC 的生成多项式，除数为 1001，被除数为 101110000，余数为 011。

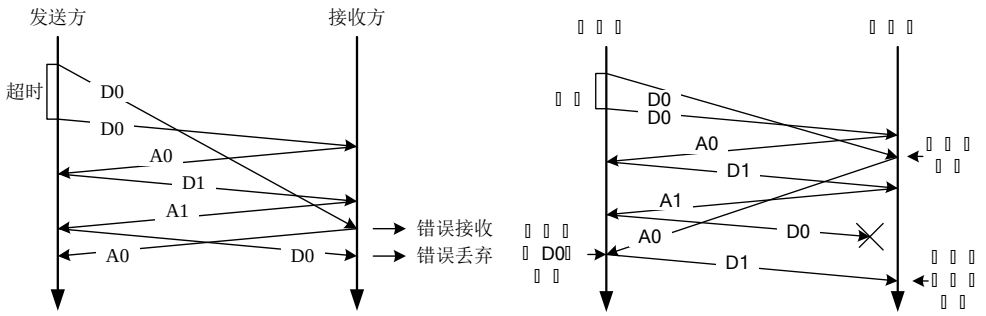
3-7 停止等待协议需不需要为确认帧编号？试举例并画图说明理由。

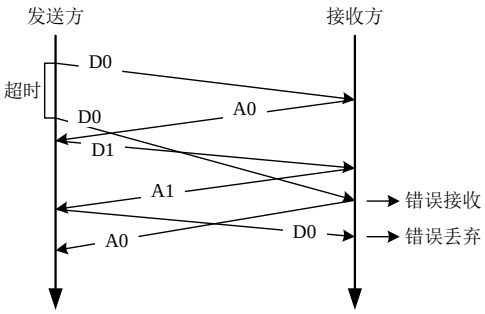
解答：在往返时延很不确定的情况下，如果确认帧不编号，当超时重传时间小于实际的往返时延时，发送方会收到重复的确认帧，导致错误，如图所示的情况，会导致 M2 丢失。但在往返时延比较确定的情况下，由于超时时间总是大于往返时延，确认帧可无需编号。




3-8 考虑 0/1 比特交替停止等待协议（序号只有一位的停止等待协议），假定发送方和接收方之间的链路会造成帧失序。请画图说明该协议将不能应对所有出错情况（协议错误地收下或丢弃数据）。

解答：如图所示，当链路造成帧失序时，0/1 编号不足以区分迟到的失序帧，会导致错误。为解决该问题需要增大编号长度。（答案不唯一）



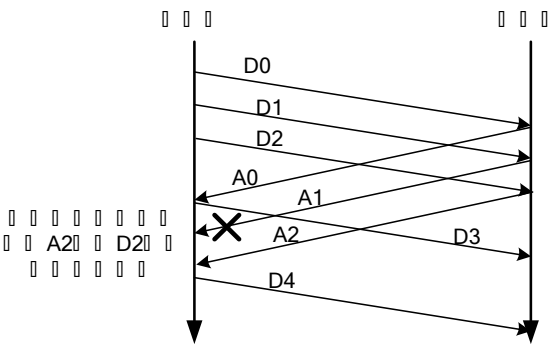

3-9 信道带宽是 4 kbit/s，传播延迟是 20 ms，那么帧的大小在什么范围内时，停止等待协议才有至少 50%的效率？

解答：帧大于 160bit。

当发送一帧的时间等于信道传播延迟的 2 倍时，信道利用率是 50%，也就是说，当发送一帧的时间等于来回路程的传播延迟时，效率是 50%。由于 20ms×2=40ms，现在发送速率是每秒 4 000bit，即发送 1bit 需要 0.25ms，40ms/(0.25ms/bit)=160bit。

3-10 判断正误：“由于 Go-Back-N 协议采用的是累积确认，当某个确认分组丢失时，不一定会导致发送方重传”，并画图举例说明。

解答：正确。



3-11 考虑 GBN 协议，当收到序号不对的分组，如果接收方仅仅将它们丢弃而不对最近按序接收的分组进行确认，会出现什么错误情况。请画图举例说明。

解答：假设窗口大小为 4，发送方连续发送 1, 2, 3, 4 号帧，接收方全部正确接收，但返回的确认帧却全部丢失。当发送方超时重传 1, 2, 3, 4 号帧时，接收方会全部丢弃（接收方正等待接收 5 号帧），如果不对 4 号帧进行再确认，发送方会一直重传 1, 2, 3, 4 号帧。（图略）

3-12 考虑在 Go-Back-N 协议中帧序号的长度问题，假设帧序号用 3 bit，而发送窗口为 8。试找出一种情况，使得在此情况下协议不能正确工作（考虑序号重用时造成的混乱，但不考虑信道失序情况）。

解答：设想在发送方的发送窗口内的序号为 0, 1, 2, 3, 4, 5, 6, 7，且全部发送出去了。而接收方的接收窗口内的序号为 0。接收端若收到 0 号帧，则无法判断是新的 0 号帧还是重传的 0 号帧（当 0 到 7 号帧的确认帧全部丢失）。

3-13 考虑选择重传协议中的上述问题，设编号用 3 bit。再设发送窗口 WT = 6 而接收窗口 WR = 3。试找出一种情况，使得在此情况下协议不能正确工作。

解答：设想在发送窗口内的序号为 0, 1, 2, 3, 4, 5，而接收窗口等待后面的 6, 7, 0。接收端若收到 0 号帧，则无法判断是新帧或重传的（当确认帧丢失）。

3-14 一条链路传输带宽为 2 Mbps，长度为 10000 km，信号传播速率为 $2.0 \times 10^5$ km/s，分组大小为 100 B，忽略应答帧大小。如果采用停止等待协议，问最大吞吐率（实际可达的最高平均数据速率）是多少？信道利用率是多少？如果采用滑动窗口协议，要想达到最高吞吐率，发送窗口最小是多少？

解答：最大吞吐率 7968 bps，信道利用率 0.3984%。如果采用滑动窗口协议，要想达到最高吞吐率，发送窗口最小为 251。

发送延迟= $(8 \times 100)/(2 \times 10^6) = 0.4$ms，传播延迟=(1000km)/(200km/ms)=50ms

1 帧发送完后等待 1 个 RTT，然后发另一帧。

周期长度=0.4ms+50ms×2=100.4ms，1 个周期内发送 1 帧。

实际数据速率=(8×100b/帧×1 帧)/100.4ms=7968bps。

信道利用率=7968bps/(2×106)bps=0.3984%。

如果采用滑动窗口协议，可连续发送的帧的个数为：

(周期长度)/(分组发送时间)=100.4ms/0.4ms=251。

所以，发送窗口最小为 251。

3-15 假定卫星信道的数据率为 100 kbps，卫星信道的单程（即从发送方通过卫星到达接收方）传输时延为 250 ms，每个数据帧长均为 2000 b，忽略误码、确认字长、首部和处理时间等开销，为达到传输的最大效率，帧的序号至少多少位？此时信道最高利用率是多少？

解答：RTT=250×2ms=0.5s

1 个帧的发送时间=2000b/100kbps= $20 \times 10^{-3}$s。

1 个帧发送完后经过 1 个单程延迟到达接收方，再经过 1 个单程延迟发送方收到应答，从而可以继续发送，理想的情况是此时窗口信息刚发送完或还没有发送完。

假设窗口值等于 x，令(2000bit×x)/(100kb/s)= $20 \times 10^{-3}$s+RTT= $20 \times 10^{-3}$s+0.5s=0.52s。

得 x=26。

若要取得最大信道利用率，窗口值是 26 即可，在此条件下，可以不间断地发送帧，所以发送率保持在 100kbps。

由于 16<26<32，帧的顺序号应为 5 位。在使用后退 N 帧协议的情况下，最大窗口值是 31，大于 26，可以不间断地发送帧，此时信道利用率是 100%。

3-16 使用 1 个 64 kbps 的卫星通道（端到端的传输延迟是 270 ms）发送 512 字节的数据帧（在一个方向上），而在另一方向上返回很短的确认帧。若滑动窗口协议的窗口大小分别为 1、7、15 和 127 时的最大吞吐率是多少？

解答：使用卫星信道，端到端的传输延迟是 270ms，以 64kbps 发送，512 字节长的数据帧占据通道的时间是$(512 \times 8)/64000 = 64 \times 10^{-3}$s，即 64ms。

用 t=0 表示传输开始时间，那么在 t=64ms 时，第 1 帧发送完毕，t=64+270=334ms 时，第 1 帧完全到达接收方，并开始返回很短的确认帧（发射时间忽略），t=334+270=604ms 时，确认帧完全到达发送方。因此，周期等于 604ms，需要窗口大小为 604/64≈9 个帧才能保持通道不空。

对于窗口值 1，每 604ms 可发送 4096 位，吞吐率=4096/0.604≈6781bps，约为 6.8kbps。

对于窗口值 7，吞吐率=6781×7=47467bps，约为 47.5kbps。

对于窗口值超过 9 帧（包括 15 帧和 127 帧的情况），吞吐率达到完全速率 64kbps。

3-17 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？

解答：PPP 协议的主要特点如下：

(1)简单，数据链路层的 PPP 协议非常简单，具有封装成帧、透明传输和差错检测功能，但向上不提供可靠传输服务。

(2)支持多种网络层协议，PPP 协议能够在在同一条物理链路上同时支持多种网络层协议，如 IP 和 IPX 等。

(3)支持多种类型链路，PPP 协议能够在多种类型的链路上运行。例如，串行的或并行的，同步的或异步的，低速的或高速的，电的或光的点对点链路。

(4)检测连接状态，PPP 协议具有一种机制能够及时（不超过几分钟）自动检测出链路是否处于正常工作状态。

(5)网络层地址协商，PPP 协议提供了一种机制使通信的两个网络层（例如，两个 IP 层）的实体能够通过协商知道或能够配置彼此的网络层地址。

帧的编号是可靠数据传输的基本机制，PPP 不使用帧的编号是因为 PPP 不实现可靠数据传输。由于 PPP 没有编号和确认机制因此不能实现可靠数据传输，适用于线路质量较好的情况。

3-18 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）？

解答：转义符为 7D，7D 5E 还原为 7E，7D 5D 还原为 7D，真正的数据为：7E FE 27 7D 7D 65 7E。

3-19 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 000111011111010111110110，问删除发送端加入的零比特后变成怎样的比特串？

解答：填充比特后为 011011111[0]11111[0]00（[]中是填充的比特）。删除比特后为 000111011111[0]11111[0]110（[]中是删除的比特）。

3-20 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？

解答：PPP 协议的工作状态有 6 种：链路静止、链路建立、鉴别、网络层协议、链路打开、链路终止。

首先要建立物理连接进入链路建立状态，然后是建立 LCP 链路，进行鉴别、NCP 配置，最后进入链路打开状态，完成数据链路层连接的建立。

3-21 局域网的主要特点是什么？为什么局域网采用广播通信方式而广域网不采用呢？

解答：局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。

由于局域网的该特点，采用广播信道方式十分简单方便。而广播通信方式需要解决共享信道问题，不利于连接覆盖地理范围非常大的大量用户，在广域范围内进行广播通信会造成通信资源的极大浪费，因此，广域网不采用广播通信方式。

3-22 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？

解答：常用的局域网的网络拓扑有星形网、环形网和总线网。现在最流行的是星形网。

3-23 什么叫做传统以太网？以太网有哪两个主要标准？

解答：由于以太网的数据率已演进到每秒百兆比特、吉比特或甚至 10 吉比特，因此通常就用“传统以太网”来表示最早流行的 10 Mbit/s 速率的以太网。

以太网有两个标准：DIX Ethernet V2 与 IEEE 的 802.3 标准。以太网是美国施乐(Xerox)公司的 Palo Alto 研究中心(简称为 PARC)于 1975 年研制成功的。1980 年 9 月，DEC 公司、英特尔(Intel)公司和施乐公司联合提出了 10 Mbit/s 以太网规约的第一个版本 DIX V1。1982 年又修改为第二版规约，即 DIX Ethernet V2，成为世界上第一个局域网产品的规约。在此基础上，IEEE 802 委员会的 802.3 工作组于 1983 年制定了第一个 IEEE 的以太网标准 IEEE 802.3，数据率为 10 Mbit/s。

3-24 试说明 10BASE-T 中的“10”、“BASE”和“T”所代表的意思。

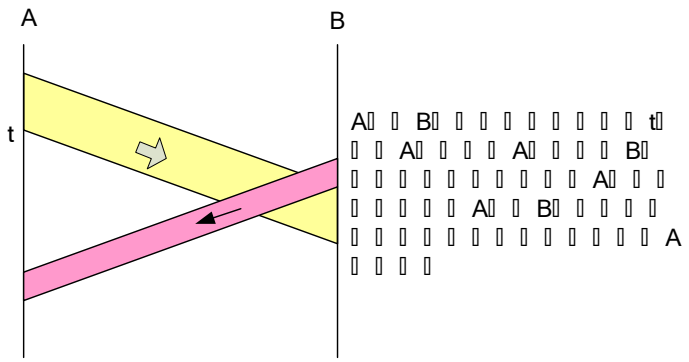
解答：“10”代表 10 Mbit/s 的数据率，BASE 表示连接线上的信号是基带信号，T 代表双绞线。

3-25 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？

解答：当网络负载较轻，各站以突发方式发送数据时，碰撞的概率很小，CSMA/CD 信道利用率和效率比较高，而 TDM 会浪费大量时隙，效率比较低。当网络负载很重时，采用 CSMA/CD 会导致大量碰撞，效率会大大下降，而 TDM 能保证每个站获得固定可用的带宽。

3-26 在以太网帧中，为什么有最小帧长的限制？画图举例说明。

解答：CSMA/CD 协议一个要点是当发送站正在发送时，若检测到冲突则立即中止发送，然后推后一段时间再发送。如果发送的帧太短，还没有来得及检测到冲突就已经发送完了，那么就无法进行冲突检测了，如图所示。因此，所发送的帧的最短长度应当要保证在发送完毕之前，必须能够检测到可能最晚来到的冲突信号。




3-27 假定 1 km 长的 CSMA/CD 网络的数据率为 1 Gbit/s。设信号在网络上的传播速率为 200000 km/s。求能够使用此协议的最短帧长。

解答：端到端往返时延为(2 km) / (200000 km/s) = 10 μs，因此只有发送时延大于该往返时延才能保证检测出所有可能的碰撞。即，最短帧长为(1 Gbit/s)× (10 μs) = 10000 bit，即 1250 字节。

3-28 假设两个结点在一个速率为 R 的广播信道上同时开始传输一个长度为 L 的分组。用 $t_{prop}$ 表示这两个结点之间的传播时延。如果 $t_{prop} > L/R$，会出现信号冲突吗（信号的叠加）？这两个结点能检测到冲突吗？为什么？通过该问题你能得到什么结论？

解答：会出现冲突。在两结点中间的某段链路上这两个结点的发送的信号必然会叠加起来，导致在该段链路上的其它结点无法正确识别信号。但这两个结点自己却无法检测到冲突，因为已经发送完了分组以后另一结点发送的信号才能到达，即在这两结点的位置并无信号的叠加。为检测出碰撞，发送时延不能太短或传播时延不能太长。

3-29 以太网不要求收到数据的目的站发回确认，为什么？

解答：因为局域网信道的质量很好，因信道质量产生差错的概率是很小的，绝大多数的差错都来自媒体访问控制中的信号冲突，这通过冲突检测和重传来解决。其他差错的纠正由上面的高层来做。收端收到有差错的帧时，丢弃即可。

3-30 有 10 个站连接到以太网上。试计算以下三种情况下每一个站所能得到的带宽。

(1) 10 个站都连接到一个 10 Mbit/s 以太网集线器；

(2) 10 个站都连接到一个 100 Mbit/s 以太网集线器；

(3) 10 个站都连接到一个 10 Mbit/s 以太网交换机。

解答：若假定利用率为 100%。(1)每个站平均得到 1 Mbit/s 带宽；(2)每个站平均得到 10 Mbit/s 带宽；(3)每个站可独占 10 Mbit/s 带宽；

3-31 有一个使用集线器的以太网，每个站到集线器的距离为 $d$，数据发送速率为 $C$，帧长为 12 500 字节，信号在线路上的传播速率为 $2.5\times10^8$ m/s。距离 $d$ 为 25 m 或 2500 m，发送速率为 10 Mbit/s 或 10 Gbit/s。这样就有 4 种不同的组合。试利用式(3-4)分别计算这 4 种不同情况下参数 $a$ 的数值，并进行简单讨论。

解答：

| | $d$ = 25 m | | $d$ = 2500 m | |
|---|---|---|---|---|
| | $C$ = 10 Mbit/s | $C$ = 10 Gbit/s | $C$ = 10 Mbit/s | $C$ = 10 Gbit/s |
| $a$ | $2\times10^{-5}$ | $2\times10^{-2}$ | $2\times10^{-3}$ | 2 |

结果表明距离越大，速率越高则参数 $a$ 越大。当帧长一定时，随着以太网的覆盖范围的增大和速率的提高，以太网的的信道利用率会降低。

3-32 公式(3-5)表示，以太网的极限信道利用率与连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连接在以太网上的站点数无关？请说明你的理由。

解答：以太网的极限信道利用率考虑的是一种最理想的情况，即假定以太网上的各站发送数据都不会产生碰撞。从概率上讲，最理想情况发生的概率极其小，因此是极限信道利用率。但实际上随着以太网上的站点数的增加，碰撞的概率会越来越大，信道的实际利用率也会越来越小。

3-33 使用 CSMA/CD 协议时，若线路长度为 100 m，信号在线路上传播速率为 $2\times10^8$ m/s。数据的发送速率为 1 Gbit/s。试计算帧长分别为 512 字节、1500 字节和 64 000 字节时的参数 $a$ 的数值，并进行简单讨论。

解答：参数 $a$ 的数值分别为：0.122，0.0417 和 0.000 977。结果表明可用通过增大以太网的帧长来提高网络的信道利用率。但帧长过大会导致发送站占用信道时间过长，而其它站等待的时间太长，会降低系统的平均响应时间。因此标准的制定需要考虑各种因素。

3-34 在以太网中，两个站发送数据冲突，不考虑其他站，它们再次冲突的概率是多少？最多两次重传就成功的概率是多少？

解答：再次冲突的概率为 50%，需要两次重传才成功的概率为 3/8 = 37.5%，因此最多两次重传就成功的概率为 87.5%。

3-35 在 CSMA/CD 中，为什么在检测到碰撞后要执行退避算法？再次重传碰撞为何要把随机选择退避时间的范围增加一倍？

解答：发生碰撞的站点不能在等待信道变为空闲后就立即再发送数据，因为会导致再次

碰撞。因此，发生碰撞的站点在停止发送数据后，要推迟（这叫作退避）一个随机的时间再监听信道进行重传。如果连续多次发生冲突，往往表明可能有较多的站点参与争用信道，需要在比较大的范围内选择退避时间才能将各站点的选择的发送时间错开，避免再次冲突。因此，当重传又发生了碰撞，则将随机选择的退避时间范围扩大一倍，以减小再次碰撞的概率。

3-36 简述局域网交换机与集线器的区别？

解答：(1)交换机工作在链路层，根据帧(链路层分组)的目的 MAC 地址进行转发；而集线器工作在物理层，仅是将端口接收到的比特转发到其他所有端口而不是对帧进行处理。(2)集线器在转发一个帧中比特时，不对传输媒体进行检测，因此其连接起来的主机属于同一冲突域；但交换机在转发一个帧之前必须执行 CSMA/CD 算法（当连接集线器时），有隔离冲突域的功能。

3-37 为什么集线器不能互连工作在不同速率的 LAN 网段，而以太网交换机却可以。

解答：集线器工作在物理层仅将电信号方大整形转发出去，不缓存整个以太网帧。而以太网交换机可以将整个以太网帧缓存到内存然后从输出端口以新的速率发送出去。

3-38 10 Mbit/s 以太网升级到 100 Mbit/s、1 Gbit/s 甚至 40/100 Gbit/s 时，都需要解决哪些技术问题？为什么以太网能够在发展的过程中淘汰掉自己的竞争对手，并使自己的应用范围从局域网一直扩展到城域网和广域网？

解答：首先是要规定新的物理层标准以提高发送速率。

其次，为了在数据发送速率提高时不降低网络的信道利用率（使参数 $a$ 仍保持不变），同时为了向后兼容，不改变以太网的帧格式和最小帧长。100 Mbit/s 以太网的争用期是 5.12 μs，帧间最小间隔现在是 0.96 μs，都是 10 Mbit/s 以太网的 1/10，将一个网段的最大电缆长度减小到 100m。而 1 Gbit/s 以太网为了不再减小最大电缆长度采用“载波延伸”和“分组突发”技术增大争用期，保持一个网段的最大电缆长度 100m。10 Gbit/s 以上以太网只工作在全双工方式，不再使用 CSMA/CD 协议，传输距离不再受碰撞检测的限制，因此可以将应用范围扩展到城域网和广域网。

以太网的以下特点使其在发展的过程中淘汰掉自己的竞争对手：

(1) 可扩展性（从 10 Mbit/s 到 40/100 Gbit/s 帧格式都保持不变）。

(2) 灵活性（支持多种媒体、全/半双工、共享/交换）。

(3) 易于安装。

(4) 稳健性好。

3-39 以太网交换机有何特点？用它怎样组成虚拟局域网？

解答：以太网交换机实质上就是一个多接口网桥，和工作在物理层的转发器和集线器有很大的差别。此外，以太网交换机的每个接口通常都直接与一个单个主机或另一个交换机相连，并且一般都工作在全双工方式。当主机需要通信时，交换机能同时连通许多对的接口，使每一对相互通信的主机都能像独占通信媒体那样，无碰撞地传输数据。以太网交换机和透明网桥一样，也是一种即插即用设备，其内部的帧转发表也是通过自学习算法自动地逐渐建立起来的，能够隔离碰撞但转发所有的广播帧。以太网交换机由于使用了专用的交换结构芯

片，其交换速率就较高。

虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。利用以太网交换机可以很方便地实现虚拟局域网 VLAN，连接到同一交换机的不同主机可以被划分到不同的 VLAN 中（最常用的技术是根据交换机的端口来划分 VLAN），这些 VLAN 在逻辑上看起来就像一些独立的 LAN，互相不能直接通信。当 VLAN 跨越多个交换机时，需要在以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记(tag)，指明发送该帧的主机属于哪一个 VLAN。

3-40　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？

解答：网桥工作在数据链路层，根据 MAC 帧的目的地址向目的主机所连接的端口进行转发，采用存储转发方式，转发时在接口执行 CSMA/CD 协议。网桥能隔离碰撞域，但转发所有的广播帧。

网桥与转发器最大的区别就是工作的层次不同。网桥工作在数据链路层，根据 MAC 帧的目的 MAC 地址进行转发；而转发器工作在物理层，用于连接电缆扩大网络覆盖范围，转发器仅仅将一个端口输入的信号放大整形转发到另一个端口，并不识别帧，也不执行 CSMA/CD 协议。

以太网交换机实质上就是一个多接口网桥，通常直接与主机或另一个交换机相连，并且一般都工作在全双工方式。而网桥通常用于将两个独立的局域网网段连接成一个局域网。

3-41　图 3-49 表示有五个站分别连接在三个局域网上，并且用网桥 B1 和 B2 连接起来。每一个网桥都有两个接口（1 和 2）。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：A 发送给 E，C 发送给 B，D 发送给 C，B 发送给 A。试把有关数据填写在表 3-3 中。

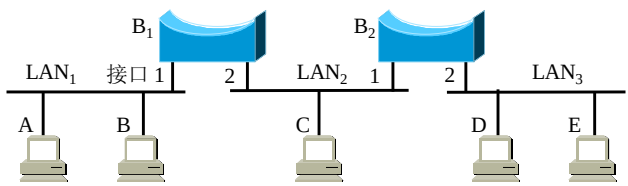



图 3-49　习题 3-41 的图

表 3-3　习题 3-41 的表

解答：

| 发送的帧 | $B_1$ 的转发表 | | $B_2$ 的转发表 | | $B_1$ 的处理 | $B_2$ 的处理 |
|---|---|---|---|---|---|---|
| | 地址 | 接口 | 地址 | 接口 | (转发？丢弃？登记？) | (转发？丢弃？登记？) |
| A → E | A | 1 | A | 1 | 转发，写入转发表 | 转发，写入转发表 |
| C → B | C | 2 | C | 1 | 转发，写入转发表 | 转发，写入转发表 |
| D → C | D | 2 | D | 2 | 写入转发表，丢弃不转发 | 转发，写入转发表 |

| | | | | | | |
|---|---|---|---|---|---|---|
| B → A | B | 1 | — | — | 写入转发表，丢弃不转发 | 接收不到这个帧 |

3-42 网桥中的转发表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？

解答：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，网桥通过向所有接口转发把数据帧正确转发到目的地址。

3-43 假设结点 A、B 和 C 都连接到同一个共享式以太网上（通过它们的适配器）。如果 A 发送上千个 IP 数据报给 B，每个封装的帧都是 B 的 MAC 地址，C 的适配器会处理这些帧吗？如果会，C 的适配器会将这些帧中的 IP 数据报传递给 C 的 IP 协议软件吗？如果 A 用 MAC 广播地址来发送帧，你的答案会有怎样的变化？

解答：第 1 问，会，因为同一个广播 LAN 上，所有适配器都会接收到这些帧，并检测该帧的目的 MAC 地址。第 2 问，不会，因为适配器仅将目的 MAC 地址为自己或广播地址的帧中的数据提交给主机。第 3 问，适配器会将广播帧中的 IP 数据报交给主机的 IP 协议软件去处理，但 C 的 IP 协议软件会丢弃该报文。

3-44 在以太网帧结构中有一个“类型”字段，简述其作用，在 PPP 帧的首部中哪个字段的功能与之最接近？

解答：该字段指明了以太网帧中的数据部分应交给哪个网络层协议或上层协议，如是 IP 协议还是 ARP 协议。PPP 帧的首部中的“协议”字段的功能与之最接近。

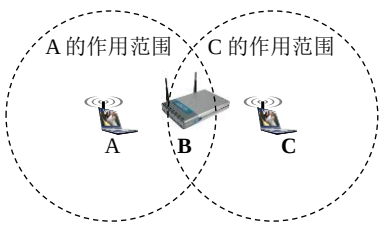
3-45 无线局域网的 MAC 协议有哪些特点？为什么在无线局域网中不能使用 CSMA/CD 协议而必须使用 CSMA/CA 协议？结合隐蔽站问题说明 RTS 帧和 CTS 帧的作用。

解答：无线局域网的 MAC 协议是 CSMA/CA（载波监听多点接入/碰撞避免）。不使用 CSMA/CD 的原因是：(1) 要实现碰撞检测，就必须在发送信号的同时接收也接收信号。这对于有线网络是很容易的事，但在无线网络中，接收信号的强度会远远小于发送信号的强度，因此实现碰撞检测的代价较大。(2) 另一方面，即使实现了碰撞检测，但由于隐蔽站问题发送站也无法检测到所有的碰撞。因此，无线局域网不使用 CSMA/CD 协议而是使用 CSMA/CA 协议，尽可能减少碰撞。由于不可能避免所有的碰撞，CSMA/CA 通过确认机制实现可靠数据传输。

无线局域网的 MAC 协议的特点是：(1)由于不实现碰撞检测，要尽可能减少碰撞。因此在监听信道时，若信道忙要执行退避算法，而不是像 CSMA/CD 一直坚持监听直到信道空闲。(2)由于不可能避免所有的碰撞，同时无线信道误码率比较高，无线局域网的 MAC 协议采用停止等待协议，保证数据链路层数据传输的可靠性。(3)为进一步减少碰撞的概率，还采用了虚拟载波监听机制，让源站把它要占用信道的时间（包括目的站发回确认帧所需的时间）及时通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据，这样就大大减少了碰撞的机会。(4)标准规定了不同长度的帧间间隔。高优先级帧需要等待的时间较短，低

优先级帧等待的时间较长。若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态因而低优先级帧就只能再推迟发送了。这样就减少了发生碰撞的机会。

隐蔽站问题如下图所示，站 A 和 C 同时向 B 发送数据。但 A 和 C 相距较远，彼此都接收不到对方发送的信号。当 A 和 C 都检测不到对方的无线信号时，就认为现在无线信道是空闲的，因而都向 B 发送数据。结果 B 同时收到 A 和 C 发来的数据，发生了碰撞。可见，在无线局域网中，即使在发送数据前未检测到传输媒体上有信号，也不能保证数据能够发送成功。为了更好地解决隐蔽站带来的碰撞问题，802.11 允许要发送数据的站对信道进行预约。源站（如 A）争取到信道后在发送数据帧之前先发送一个短的控制帧，叫做请求发送 RTS（Request To Send），它包括源地址、目的地址和这次通信（包括相应的确认帧）所需的持续时间。若目的站（如 B）正确收到源站发来的 RTS 帧，且媒体空闲，就发送一个响应控制帧，叫做允许发送 CTS (Clear To Send)，它也包括这次通信所需的持续时间（从 RTS 帧中将此持续时间复制到 CTS 帧中）。源站收到 CTS 帧后，再等待一段时间 SIFS 后发送其数据帧。若目的站正确收到了源站发来的数据帧，在等待时间 SIFS 后，就向源站发送确认帧 ACK。在 A 的作用范围内的所有其他站监听到 RTS 后，执行虚拟载波监听，在 A 和 B 通信期间不会发送数据。在 A 的作用范围外，但在 B 的作用范围内的其他站（如 C），虽然收不到 A 的 RTS，但能收到 B 的 CTS，因此 C 知道 A 和 B 将要通信，并在 A 和 B 通信期间也不会发送数据。



A 和 C 同时向 B 发送信号，发生碰撞

3-46　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？

解答：由于无线局域网的 MAC 协议不进行碰撞检测，而且无线信道易受干扰，导致大量帧因为碰撞或其他干扰不能被目的站正确接收，因此在无线局域网上发送数据帧后要对方必须发回确认帧，若超时收不到确认，则进行重传。而在以太网有线网络中，可以很容易实现碰撞检测，当信号碰撞时能及时检测到并进行重传。而如果信号不碰撞，在有线网络中误码率是非常低的，因此没有必要实现可靠数据传输。

3-47　802.11 的 MAC 协议中的 SIFS 和 DIFS 的作用是什么？

解答：标准规定两种长度的帧间间隔是为了实现不同类型帧的发送优先级。高优先级帧等待的时间较短，低优先级帧等待的时间较长。若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态因而低优先级帧就只能再推迟发送了。

SIFS，即短帧间间隔，用来分隔开属于一次对话的各帧，保证一次会话不会被低优先级的帧所打断。使用 SIFS 的帧类型有 ACK 帧、CTS 帧（在本节后面有介绍）、由过长的 MAC 帧分片后的数据帧，以及所有回答 AP 探询的帧和在 PCF 方式中接入点 AP 发送出的任何帧。

DIFS，即分布协调功能帧间间隔，它比 SIFS 的帧间间隔要长得多，在 DCF 方式中用来发送数据帧和管理帧。

3-48 试解释无线局域网中的名词：BSS、ESS、AP、DCF 和 NAV。

解答：

BSS (Basic Services Set)，基本服务集，是无线局域网的最小构件。一个基本一个 BSS 包括一个基站和若干个移动站。

ESS (Extended Service Set)，扩展的服务集。一个基本服务集可以通过接入点 AP 连接到一个分配系统 DS (Distribution System)，然后再连接到另一个基本服务集，这样就构成了一个扩展的服务集。

AP (Access Point)，接入点，就是基本服务集 BSS 中的基站。所有站要和本 BSS 以外的站通信时都必须通过本 BSS 的基站，一个基本服务集可以通过接入点 AP 连接到一个分配系统 DS (Distribution System)，然后再连接到另一个基本服务集，这样就构成了一个扩展的服务集。

DCF (Distributed Coordination Function)，分布协调功能。802.11 的 MAC 层包括两个子层。在下面的一个子层是分布协调功能。DCF 向上提供争用服务，让各个站通过争用信道来获取发送权。

NAV (Network Allocation Vector)，网络分配向量，是一个各站维护的内部状态变量，指出信道处于忙状态的持续时间。当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 NAV。

3-49 Wi-Fi 和 WLAN 是完全相同的意思吗？请简单说明一下。

解答：在概念上并不完全相同。Wi-Fi（Wireless Fidelity，即无线保真度）是 IEEE 802.11 无线局域网的代名词。从理论上讲，不采用 IEEE 802.11 标准的无线局域网不能称为 Wi-Fi，但实际上目前流行的无线局域网都是 IEEE 802.11 系列标准。因此，在当前，Wi-Fi 几乎成为了无线局域网 WLAN 的同义词。

## 第 4 章

4-1 网络层向上提供的服务有哪两种？试比较其优缺点。

解答：面向连接的虚电路服务和无连接的数据报服务。

| 对比的方面 | 虚电路服务 | 数据报服务 |
|---|---|---|
| 思路 | 可靠通信应当由网络来保证 | 可靠通信应当由用户主机来保证 |
| 连接的建立 | 必须有 | 不需要 |
| 终点地址 | 仅在连接建立阶段使用，每个分组使用短的虚电路号 | 每个分组都有终点的完整地址 |
| 分组的转发 | 属于同一条虚电路的分组均按照同一路由进行转发 | 每个分组独立选择路由进行转发 |
| 当结点出故 | 所有通过出故障的结点的虚电 | 出故障的结点可能会丢失分组，一 |

| | | |
|---|---|---|
| 障时 | 路均不能工作 | 些路由可能会发生变化 |
| 分组的顺序 | 总是按发送顺序到达终点 | 到达终点时不一定按发送顺序 |
| 端到端的差错处理和流量控制 | 可以由网络负责，也可以由用户主机负责 | 由用户主机负责 |

4-2 请简述网络层的转发和选路两个重要功能的区别和联系。

答：转发指从路由器的输入链路接收分组，根据转发表选择适当的路由器输出链路输出。选路涉及一个网络中的所有路由器，它们集体地通过选路协议交互，决定分组从源到目的地所采用的路由。选路算法最终生成转发所用的转发表。

4-3 虚电路服务与数据报服务的产生背景有什么不同？它们对网络结构有何影响？

答：虚电路服务的思路来源于传统的电信网。电信网将其用户终端（电话机）做得非常简单，而电信网负责保证可靠通信的一切措施，因此电信网的结点交换机复杂而昂贵。数据报服务使用另一种完全不同的新思路。它力求使网络生存性好和使对网络的控制功能分散，因而只能要求网络提供尽最大努力的服务。但这种网络要求使用较复杂且有相当智能的主机作为用户终端。可靠通信由用户终端中的软件（即 TCP）来保证。

4-4 在虚电路网络中为什么一个分组沿其路径的每条链路上不能保持相同的虚电路号？

答：(1)逐链路 VC 号代替统一号码减少了在分组首部 VC 字段的长度。(2)更重要的是，该方法大大简化了虚电路的建立，每段链路的 VC 号独立选择，无须所有路由器互相交互信息选择一个全局唯一的 VC 号。

4-5 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？

解答：虽然让所有用户使用相同的网络，会使网络互连变得非常简单，但实际上是不可行的。因为用户的需求是多种多样的，没有一种单一的网络能够适应所有用户的需求。另外，网络技术是不断发展的，网络的制造厂家也要经常推出新的网络，要在竞争中求生存。因此在市场上总是有很多种不同性能、不同网络协议的网络，供不同的用户选用。我们面临的现实就是：在客观上，世界上有很多特性各异的网络，但这些网络又希望能够相互通信，因此网络互连的意义非常重要。

互连在一起的网络要进行通信，会遇到许多问题需要解决，如：

不同的寻址方案；

不同的最大分组长度；

不同的网络接入机制；

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。

4-6 作为中间设备，转发器、网桥、路由器和网关有何区别？

解答：(1) 物理层使用的中间设备叫做转发器(repeater)。

(2) 数据链路层使用的中间设备叫做网桥或桥接器(bridge)。

(3) 网络层使用的中间设备叫做路由器(router)。

(4) 在网络层以上使用的中间设备叫做网关(gateway)。用网关连接两个不兼容的系统需要在高层进行协议的转换。

4-7 试简单说明下列协议的作用：

IP, ARP 和 ICMP。

解答：网际协议 IP 用于互连异构网络，运行在主机和互连异构网络的路由器上，使这些互连的异构网络在网络层上看起来好像是一个统一的网络。

地址解析协议 ARP 用来把一个机器的 IP 地址解析为相应的物理地址。

互联网控制报文协议 ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。

4-8 为什么 ARP 查询要在广播帧中发送，而 ARP 响应要用单播帧？

解答：由于查询方不知道被查询方的 MAC 地址（这也正是为何要进行 ARP 查询的原因），而所有结点都要处理广播帧，因此通过广播发送给被查询方。而被查询方通过接收到的广播帧的源地址知道查询方的 MAC 地址了，因此可以用该地址进行响应，这样局域网中的除查询方外其它主机就不会接收和处理该 ARP 响应了，避免浪费带宽和其它主机的计算资源。

4-9 分类 IP 地址分为哪几类？各如何表示？IP 地址的主要特点是什么？

解答：IP 地址分为五类：

A 类地址：网络号前 8 位，第 1 位为 0；

B 类地址：网络号前 16 位，前 2 位为 10；

C 类地址：网络号前 8 位，前 3 位为 110；

D 类地址：网络号前 8 位，前 4 位为 1110；

E 类地址：网络号前 8 位，前 4 位为 1111。

IP 地址具有以下一些重要特点：

(1) 每一个 IP 地址都由网络号和主机号两部分组成。从这个意义上说，IP 地址是一种分等级的地址结构。

(2) 实际上 IP 地址是标志一个主机（或路由器）和一条链路的接口。

(3) 按照因特网的观点，一个网络是指具有相同网络号 net-id 的主机的集合，因此，用转发器或网桥连接起来的若干个局域网仍为一个网络，因为这些局域网都具有同样的网络号。具有不同网络号的局域网必须使用路由器进行互连。

(4) 在 IP 地址中，所有分配到网络号的网络(不管是范围很小的局域网，还是可能覆盖很

大地理范围的广域网)都是平等的。

4-10 对于分类编址方式，分别计算 A、B、C 三类网络各自可容纳的主机数量。

解答：A:16777214; B:65534;C:254。

4-11 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？

解答：从层次的角度看，物理地址是数据链路层和物理层使用的地址，而 IP 地址是网络层和以上各层使用的地址，是一种逻辑地址（称 IP 地址是逻辑地址是因为 IP 地址是用软件实现的）。

由于世界上已经存在各式各样的网络，它们使用不同的硬件地址，为了互连这些使用不同硬件地址的网络，需要在上层使用一种统一的逻辑地址，即 IP 地址。因此，当在一个物理网络中进行通信时，要使用该网络网络的硬件地址，而要跨多个网络进行通信时就必须使用 IP 地址。另外，数据链路层和网络层使用不同的地址，可以保持各层的独立性，底层物理网络可以采用任何技术，并可以支持其他网络层协议（如：IPX、DECnet 等）。

4-12 试辨认分类编址方式中以下 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

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

4-13 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？

解答：好处：转发分组更快。缺点：数据部分出现差错时不能及早发现。

4-14 简述 IP 数据报首部中的寿命字段（TTL）的作用。

解答：该字段指明了该数据报还能经过多少个路由器的转发，每次数据报经过一台路由器时，该字段的值减 1。若 TTL 字段减为 0，则该数据报被丢弃，不再进行转发因此该字段用来确保数据报不会永远在网络中循环（可能由于路由表的错误）。

4-15 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？

解答：IP 协议不实现可靠数据传输，IP 协议没有重传机制。同时，源地址字段也可能出错，以致无法找到源站。

虽然 CRC 的检错能力更强，但因特网校验和算法比 CRC 更易于用软件实现，并且计算更快，而 CRC 更适合用硬件来实现，因此在数据链路层通常使用 CRC，但在 IP 协议中却不

采用 CRC，以减轻路由器的负担。

4-16 什么是最大传送单元 MTU？它和 IP 数据报首部中的哪个字段有关系？

解答：在 IP 层下面的每一种数据链路层都有其自己的帧格式，其中包括帧格式中的数据字段的最大长度，这称为最大传送单元 MTU (Maximum Transfer Unit)。当一个 IP 数据报封装成链路层的帧时，此数据报的总长度（即首部加上数据部分，IP 首部中总长度字段）一定不能超过下面的数据链路层的 MTU 值。

4-17 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。

解答：在目的站组装的好处有以下几点。

（1）减轻路由器的工作负担。

（2）由于每个数据报片都是独立路由的，并非所有的数据报片都经过同样的路由器。

（3）也许分组后面还要经过一个网络，它还要将这些数据报片划分成更小的片。

4-18 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 比特。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）？

解答：由于分片，共分为 4 个数据报片，故第二个局域网向上传送 3840 字节的数据（4 个分片 IP 报文的总长度）。

4-19 回答以下有关 ARP 的问题：

(1) 有人认为：“在因特网中，当计算机 A 要与计算机 B 通信时，若 A 不知道计算机 B 的物理地址，要先通过 ARP 将 B 的 IP 地址解析为物理地址，然后再利用该物理地址向 B 发送报文。”这种说法正确吗？

(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目的 IP 地址解析为相应的硬件地址）。

解答：(1) 不对：当 A 和 B 不在一个局域网中时，A 发送给 B 的 IP 报文需要中间路由器转发，A 需要通过 ARP 解析中间路由器的物理地址，而不是 B 的物理地址。

(2) 当网络中某个 IP 地址和硬件地址的映射关系发生变化时，ARP 高速缓存中的相应项目就要改变（例如，更换网卡等）。实践证明缓存超时时间设置为 10 ~ 20 分钟较为合理，太短会导致 ARP 请求过于频繁，而太长会导致更换网卡的主机不能及时与其它主机通信。

(3) 当 ARP 高速缓存已有该 IP 地址项目，或广播分组

4-20 主机 A 发送 IP 数据报给主机 B，途中经过了 5 个路由器（若连接的都是局域网）。试问在 IP 数据报的发送过程中总共使用了几次 ARP?

解答：若连接的都是局域网，则需要 6 次。

4-21 某单位分配到地址块 129.250.0.0/20。该单位有 4000 台机器，平均分布在 16 个不同的地点。试给每一个地点分配一个网络地址和子网掩码，并算出每个地点能分配给主机的 IP 地址的最小值和最大值。

解答：给每一个地点分配子网掩码 255.255.255.0，每个子网有 254 个可分配地址。4000 多台计算机分布在 16 不同地点，所以每个地点最多 254 台电脑。每个地点的网络前缀和主机 IP 地址的最小值和最大值为:

129.250.0.0/24: 129.250.0.1~129.250.0.254

129.250.1.0/24: 129.250.1.1~129.250.1.254

129.250.2.0/24: 129.250.2.1~129.250.2.254

129.250.3.0/24: 129.250.3.1~129.250.3.254

……

129.250.15.0/24: 129.250.15.1~129.250.15.254

4-22 一个数据报长度为 4000 字节（固定首部长度）。现在经过一个网络传送，但此网络能够传送的最大数据长度为 1500 字节。试问应当划分为几个短些的数据报片？各数据报片的数据字段长度、片偏移字段和 MF 标志应为何数值？

解答：分片前数据部分长度：4000-20=3980。分片后每片数据不能超过：1500-20=1480。由于 1480 正好能被 8 整除，因此每片数据最大长度为 1480。

共分为 3 个数据报片。数据字段长度分别为 1480, 1480 和 1020 字节。

片偏移字段的值分别为 0，185 和 370。MF 字段的值分别为 1, 1 和 0。

4-23 路由器转发 IP 数据报的基本过程。

解答：在划分子网的情况下，路由器转发分组的算法如下：

(1)从收到的数据报首部提取目的 IP 地址 D。

(2)先判断是否为直接交付。对路由器直接相连的网络逐个进行检查：用各网络的掩码和 D 逐位相“与”（AND 操作），看结果是否和相应的网络地址匹配。若匹配，则把分组进行直接交付（当然还需要把 D 转换成物理地址，把数据报封装成帧发送出去），转发任务结束。否则就是间接交付，执行(3)。

(3)对路由表中的每一行（网络地址，掩码，下一跳，接口），用其中的掩码和 D 逐位相“与”（AND 操作），其结果为 N。若 N 与该行的网络地址匹配，则把数据报传送给该行指明的下一跳路由器；否则，执行(4)。

(4)若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(5)。

(5)报告转发数据报出错。

4-24 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个地址？如果有，请指出，并说明理由。

解答：前一个地址块包含了后一个。写出这两个地址块的二进制表示就可看出。

4-25 有如下的 4 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

解答：共同的前缀有 22 位，即：11010100 00111000 1000001。

聚合的 CIDR 地址块是：212.56.132.0/22。

4-26 某主机的 IP 地址是 227.82.157.177/20。试问该主机所连接的网络的网络前缀是什么？该网络的网络地址是什么？主机号占多少位？主机号的二进制表示是什么？

解答：网络前缀是：11100011 01010010 1001，或用十进制表示为：227.82.144.0/20。

网络地址是：11100011 01010010 10010000 00000000，或用十进制表示为：227.82.144.0。

主机号占 12 位，其二进制这表示是：1101 10110001。

4-27 设某路由器建立了如表 4-8 所示的路由表（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）：

**表 4-8** 某路由器的路由表

| 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 | $R_2$ |
| 192.4.153.0 | 255.255.255.192 | $R_3$ |
| *（默认） | — | $R_4$ |

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

试分别计算这些分组转发的下一跳。

解答：(1)接口 0; (2) R2; (3) R4; (4) R3; (5) R4。

4-28 考虑某路由器具有下列路由表项：

**表 4-9** 某路由器的路由表

| 网络前缀 | 下一跳 |
|---|---|

| | |
|---|---|
| 142.150.64.0/24 | A |
| 142.150.71.128/28 | B |
| 142.150.71.128/30 | C |
| 142.150.0.0/16 | D |

（1）假设路由器接收到一个目的地址为 142.150.71.132 的 IP 分组，请确定该路由器为该 IP 分组选择的下一跳，并解释说明。

（2）在上面的路由表中增加一条路由表项，该路由表项使以 142.150.71.132 为目的地址的 IP 分组选择“A”作为下一跳，而不影响其他目的地址的 IP 分组转发。

（3）在上面的路由表中增加一条路由表项，使所有目的地址与该路由表中任何路由表项都不匹配的 IP 分组被转发到下一跳“E”。

（4）将 142.150.64.0/24 划分为 4 个规模尽可能大的等长子网，给出子网掩码及每个子网的主机 IP 地址范围。

解答：（1）B；（2）<142.150.71.132/32, A>；（3）<0.0.0.0/0, E>；

（4）子网掩码 255.255.255.192，

142.150.64.1~142.150.64.62, 142.150.64.65~142.150.64.126,

142.150.64.129~142.150.64.190, 142.150.64.193~142.150.64.254

4-29 如图 4-57 所示，某单位有两个局域网（各有 120 台计算机），通过路由器 R2 连接到因特网，现获得地址块 108.112.1.0/24，为这两个局域网分配 CIDR 地址块，并为路由器 R2 的接口 1、接口 2 分配地址（分配最小地址）。配置 R2 的路由表（目的地址，子网掩码，下一跳），在 R1 的路由表中增加一条项目使该单位的网络获得正确路由。

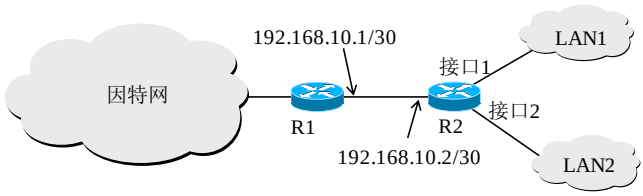



图 4-57 习题 4-29 的图

解答：LAN1: 108.112.1.0/25; LAN2: 108.112.1.128/25; 接口 1: 108.112.1.1; 接口 2: 108.112.1.129（或 LAN1，LAN2 互换）

R2 路由表：

| 目的地址 | 子网掩码 | 下一跳 |
|---|---|---|
| 108.112.1.0 | 255.255.255.128 | 接口 1(直接交付) |
| 108.112.1.128 | 255.255.255.128 | 接口 2(直接交付) |
| 192.168.10.0 | 255.255.255.252 | 直接交付 |
| *(默认路由)0.0.0.0 | 0.0.0.0 | 192.168.10.1 |

通过路由聚合，给 R1 的路由表增加：(108.112.1.0, 255.255.255.0, 192.168.10.2)。

4-30 一个自治系统有 5 个局域网，其连接图如图 4-58 示。LAN2 至 LAN5 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）。

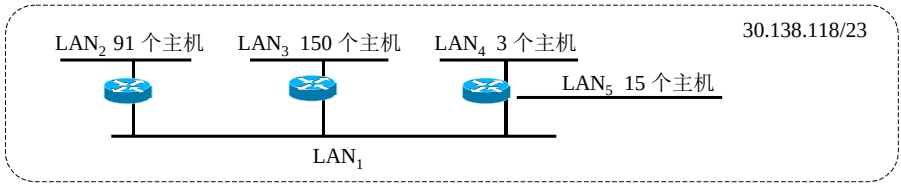



图 4-58 习题 4-30 的图

解答：本题的解答并不唯一，以下是其中两种方案：

LAN1：30.138.119.192/29
LAN2：30.138.119.0/25
LAN3：30.138.118.0/24
LAN4：30.138.119.200/29
LAN5：30.138.119.128/26

LAN1：30.138.118.192/27
LAN2：30.138.118.0/25
LAN3：30.138.119.0/24
LAN4：30.138.118.224/27
LAN5：30.138.119.128/27

若按“先分大网再分小网，划分大小最合适的地址块，允许剩余地址块”的原则划分，得到以下唯一方案：

LAN1：30.138.119.168/29
LAN2：30.138.119.0/25
LAN3：30.138.118.0/24
LAN4：30.138.119.160/29
LAN5：30.138.119.128/27

4-31 已知某地址块中的一个地址是 140.120.84.24/20。试问该地址块中的第一个地址是什么？这个地址块共包含有多少个地址？最后一个地址是什么？

解答：第一个地址：140.120.80.0。地址块中的地址数是 4096 个。最后一个地址：140.120.95.255。

4-32 某主机的 IP 地址为 140.252.20.68，子网掩码为 255.255.255.224，计算该主机所在子网的网络前缀（采用 CIDR 地址表示法 a.b.c.d/x），该子网的地址空间大小和地址范围（含特殊地址）。

解答：140.252.20.64/27，32, 140.252.20.64 至 140.252.20.95

4-33 某组织分配到一个地址块，其中的第一个地址是 14.24.74.0/24。这个组织需要划分

为 11 个子网。具体要求是：具有 64 个地址的子网 2 个；具有 32 个地址的子网 2 个；具有 16 个地址的子网 3 个；具有 4 个地址的子网 4 个（这里的地址都包含全 1 和全 0 的主机号）。试设计这些子网。分配结束后还剩下多少个地址？

解答：具有 64 个地址的子网是：14.24.74.0/26，14.24.74.64/26。

具有 32 个地址的子网是：14.24.74.128/27，14.24.74.160/27。

具有 16 个地址的子网是：14.24.74.192/28，14.24.74.208/28，14.24.74.224/28。

具有 4 个地址的子网是：14.24.74.240/30，14.24.74.244/30，14.24.74.248/30，14.24.74.252/30。

全部 256 个地址已经分配完毕，没有剩下的地址。

4-34 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。

解答：只有(1)是匹配的。

4-35 以下的地址前缀中的哪一个地址和 2.52.90.140 匹配？请说明理由。

(1) 0/4; (2) 32/4; (3) 4/6; (4) 80/4。

解答：只有(1)是匹配的。

4-36 IGP 和 EGP 这两类协议的主要区别是什么？

解答：(1) 内部网关协议 IGP (Interior Gateway Protocol)　即在一个自治系统内部使用的路由选择协议，而这与在互联网中的其他自治系统选用什么路由选择协议无关。目前这类路由选择协议使用得最多，如 RIP 和 OSPF 协议。

(2) 外部网关协议 EGP (External Gateway Protocol)　若源主机和目的主机处在不同的自治系统中（这两个自治系统可能使用不同的内部网关协议），当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中。

4-37 考虑 RIP，假定网络中的路由器 B 的路由表有如下的项目（目的网络、距离、下一跳）

| | | |
|---|---|---|
| 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（目的网络、距离）：(N2, 4)、(N3, 8)、(N6, 4)、(N8, 3)、(N9, 5)，试求路由器 B 更新后的路由表（详细说明每项的原因）。

解答：

| | | | |
|---|---|---|---|
| N1 | 7 | A | 无新信息，不变 |
| N2 | 5 | C | 相同下一跳，更新 |
| N3 | 9 | C | 新项目，增加 |
| N6 | 5 | C | 不同下一跳，距离更短，更新 |

| | | | |
|---|---|---|---|
| N8 | 4 | E | 不同下一跳，距离一样，不变 |
| N9 | 4 | F | 不同下一跳，距离更大，不变 |

4-38 考虑 RIP，假定网络中的路由器 A 的路由表有如下的项目（目的网络、距离、下一跳）

| | | |
|---|---|---|
| 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（目的网络、距离）: (N1, 2)、(N2, 1)、(N3, 3)、(N4, 7)，试求路由器 A 更新后的路由表（详细说明每项的原因）。

解答：

| | | | |
|---|---|---|---|
| N1 | 3 | C | 不同下一跳，距离更短，更新 |
| N2 | 2 | C | 相同下一跳，距离一样，不变 |
| N3 | 1 | F | 不同下一跳，距离更大，不变 |
| N4 | 5 | G | 不同下一跳，距离更大，不变 |

4-39 试简述 RIP, OSPF 和 BGP 路由选择协议的主要特点。

解答：RIP 协议采用距离向量算法，其特点是：

(1) 仅和相邻路由器交换信息。如果两个路由器之间的通信不需要经过另一个路由器，那么这两个路由器就是相邻的。RIP 协议规定，不相邻的路由器不交换信息。

(2) 路由器交换的信息是当前本路由器所知道的全部信息，即自己的路由表。也就是说，交换的信息是：“我到本自治系统中所有网络的（最短）距离，以及到每个网络应经过的下一跳路由器”。

(3) 按固定的时间间隔交换路由信息，例如，每隔 30 秒。然后路由器根据收到的路由信息更新路由表。当网络拓扑发生变化时，路由器也及时向相邻路由器通告拓扑变化后的路由信息。

OSPF 协议采用链路状态算法，其特点是：

(1) 向本自治系统中所有路由器发送信息。这里使用的方法是洪泛法(flooding)，这就是路由器通过所有输出端口向所有相邻的路由器发送信息。而每一个相邻路由器又再将此信息发往其所有的相邻路由器（但不再发送给刚刚发来信息的那个路由器）。这样，最终整个区域中所有的路由器都得到了这个信息的一个副本。

(2) 发送的信息就是与本路由器相邻的所有路由器的链路状态，但这只是路由器所知道的部分信息。所谓 “链路状态”就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”(metric)。OSPF 将这个“度量”用来表示费用、距离、时延、带宽，等等。这些都由网络管理人员来决定，因此较为灵活。为了方便就称这个度量为“代价”。

(3) 只有当链路状态发生变化时，路由器才向所有路由器用洪泛法发送此信息。而不像 RIP 那样，不管网络拓扑有无发生变化，路由器之间都要定期交换路由表的信息。

(4) 对于规模很大的网络，OSPF 可以把一个自治系统再划分为若干个更小范围的区域

(area)，实现层次路由。

BGP 协议采用路径向量算法，其特点是：

(1) BGP 在自治系统之间交换交换“可达性”信息（即“可到达”或“不可到达”），而不是用“代价”作为度量来寻找最佳路由。例如，告诉相邻路由器：“到达目的网络 N 可经过 ASx”。

(2) AS 之间的路由选择必须考虑有关策略。这些策略包括政治、安全或经济方面的考虑。

(3) 边界网关协议 BGP 只是力求寻找一条能够到达目的网络且比较好的路由（不能兜圈子），而并非要寻找一条最佳路由。

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 周期性地和邻站交换路由信息而 BGP 却不这样做？

解答：RIP 只和邻站交换信息，UDP 虽不保证可靠性，但 UDP 开销小。

OSPF 使用可靠的洪泛法，并直接使用 IP，好处是灵活和开销小。

BGP 需要交换自治系统间的路由信息，交换的信息大，使用 TCP 提供可靠交付。

RIP 使用不可靠的 UDP，因此需要周期性地和邻站交换路由信息，而 BGP 不需要。

4-41 为何 BGP 可以避免“坏消息传播得慢”的问题？

解答：因为当一个路由器通过 BGP 会话通告一个前缀时，该前缀的 BGP 属性中包含该前缀通告通过的 AS 路径，若路由器在该路径中发现自己的 AS 包含在该路径中，则拒绝该通告，从而防止循环通告和选路环路，因此可以避免“坏消息传播得慢”的问题。

4-42 比较交换机和路由器各自的特点和优缺点。

解答：路由器是利用网络层地址转发分组的存储转发分组交换机。尽管交换机也是一个存储转发分组交换机，它和路由器根本不同，因为它用 MAC 地址转发分组。交换机是第二层的分组交换机，而路由器是一个第三层的分组交换机。

交换机的优点：交换机是即插即用的。交换机还能够具有相对高的分组过滤和转发率（交换机只需处理通过第二层传送上来的分组，而路由器必须处理通过第三层传送上来的帧）。

交换机的缺点：由于 MAC 地址是平坦的，一个大型交换机网络要求交换机维护大的转发表，也将要求在主机中维护大的 ARP 表，将产生和处理大量的 ARP 流量。交换机对于广播风暴不提供任何保护措施，如果一台主机失去控制并传输了无穷的以太网广播帧流，交换机将转发所有这些帧，导致整个以太网的崩溃。交换机网络的拓扑结构限制为一棵生成树。

路由器的优点：分组就不会被限制在一棵生成树上，并且可以使用源和目的之间的最佳路径。因为网络寻址经常是层次的（不像 MAC 寻址那样是平面的），即使当网络中存在冗余路径，分组通常也不会在路由器中循环。（当路由器表配置有问题时，分组可能会循环；但 IP 用一个特殊的报文首部字段来限制循环。）路由器为第二层的广播风暴提供了隔离保护。

路由器的缺点：路由器不是即插即用的（它们以及连接到它们的主机都需要配置 IP 地址）。路由器对每个分组处理时间通常比交换机更长。因为它们必须处理到第三层的字段。

4-43 路由器的输入端口和输出端口都有排队功能，什么情况下分组会在输入端口排队，

而什么情况下分组会在输出端口排队？如果能让路由器处理分组足够快，是否能使输入和输出端口都避免出现分组排队（假定输入/输出线路速率相同）？

解答：如果路由器的交换结构的速率跟不上所有输入端口分组的到达速率时，分组会因为等待交换而在输入队列中排队。当交换结构传送过来的分组的速率超过输出链路的发送速率时，来不及发送的分组就必须暂时存放在这个队列中。提高路由器查表和交换的速度可以避免分组在输入端口进行排队，但不能完全避免在输出端口的排队。

4-44 简述 IGMP 和多播选路协议的作用。

答：IGMP 和多播选路协议是因特网实现网络层多播的两个互补的组件：

IGMP 通知本地的多播路由器有主机参与某多播组。

多播选路协议用于本地多播路由器与其他多播路由器联系，传送组成员关系信息，建立多播路由。

4-45 什么是可重用地址和专用地址？什么是虚拟专用网 VPN？

解答：RFC 1918 指明了一些专用地址。这些地址只能用于一个机构的内部通信，而不能用于和因特网上的主机通信。换言之，专用地址只能用作本地地址而不能用作全球地址。在因特网中的所有路由器，对目的地址是专用地址的数据报一律不进行转发。显然，不同机构的专用互连网络可以使用相同的专用 IP 地址，因此专用 IP 地址也叫做可重用地址。

利用公用的因特网作为本机构各专用网之间的通信载体，这样的专用网又称为虚拟专用网。“专用网”是因为这种网络是为本机构的主机用于机构内部的通信，而不是用于和网络外非本机构的主机通信。“虚拟”表示“好像是”，但实际上并不是，因为现在并没有使用专线而是通过公用的因特网来连接分散在各场所的本地网络。

4-46 内联网(Intranet)和外联网(Extranet)是怎样的网络？它们的区别是什么？

解答：由一个机构的几个内部网络所构成的虚拟专用网 VPN 又称为内联网(intranet 或 intranet VPN，即内联网 VPN)，表示这些网络都属于同一个机构。

有时一个机构的 VPN 需要有某些外部机构（通常就是合作伙伴）参加进来。这样的 VPN 就称为外联网(extranet 或 extranet VPN，即外联网 VPN)。

4-47 考虑图 4-41 中的基本 NAT 方法，假设 NAT 路由器只拥有 1 个全球 IP 地址，若有多台专网主机想同时访问因特网上资源会出现什么问题？当采用 NAPT 情况有会怎样？

解答：会发生冲突，不能都成功通信。因为，同一时刻只能有一台专网主机访问因特网上的主机。NAT 路由器无法区分返回的 IP 数据报是发送给谁的。

当采用 NAPT 时，NAPT 路由器将运输层的端口号和 IP 地址一起进行转换，并利用端口号来区分不同的报文。由于端口号字段有 16 比特，因此一个外部 IP 地址可支持 60000 多对内部进程（可位于不同主机）与外部进程的通信。

4-48 因特网的多播是怎样实现的？为什么因特网上的多播比以太网上的多播复杂得多？

解答：首先是使用多播地址来标识多播分组的接收方，即多播组。另外，需要使用两种协议：一个是 IGMP 协议，让连接在本地局域网上的多播路由器知道本局域网上是否有主机（严格讲，是主机上的某个进程）参加或退出了某个多播组。

显然，仅有 IGMP 协议是不能完成多播任务的。连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便把多播数据报用最小代价传送给所有的组成员。这就需要使用多播路由选择协议。

由于以太网是一个广播网，利用广播很容易实现多播。交换机转发所有多播帧（目的地址是多播地址的帧）就可以将帧发送给以太网上所有主机，而收到帧的适配器通过识别目的组地址来过滤掉不需要接收的帧。而在因特网上实现多播要复杂得多，因为在因特网范围内进行广播是灾难性的。为减少分组不必要的转发，需要生成多播转发树（连接多播组成员的树），多播路由器仅在多播转发树上进行转发。多播转发树必须动态地适应多播组成员的变化。因为，因特网上的多播比以太网上的多播复杂得多。

4-49 IP 多播为什么需要两种协议？这两种协议各自的主要功能是什么？

解答：IGMP 协议是让连接在本地局域网上的多播路由器知道本局域网上是否有主机（严格讲，是主机上的某个进程）参加或退出了某个多播组。仅有 IGMP 协议是不能完成多播任务的。连接在局域网上的多播路由器还必须和因特网上的其他多播路由器协同工作，以便把多播数据报用最小代价传送给所有的组成员。这就需要使用多播路由选择协议。

多播路由选择协议的基本任务就是在多播路由器之间为每个多播组建立一个连接源和所有拥有该组成员的路由器的多播转发树。IP 多播数据报只要沿着多播转发树进行洪泛就能被传送到所有的拥有组成员的多播路由器，然后在局域网内多播路由器再通过硬件多播将 IP 多播数据报发送给所有组成员。

4-50 为什么 IGMP 要使用 IP 多播进行传输，并且其 IP 数据报的 TTL 被设置为 1？

解答：为了提高 IGMP 的工作效率，减少组成员和多播路由器发送 IGMP 报文的数量，IGMP 报文使用 IP 多播进行传输。例如，延迟响应和选择查询路由器都需要多播的支持。同时，IGMP 仅用于在本地网络中组成员向多播路由器通告成员关系，为了避免封装了 IGMP 报文的 IP 多播数据报被路由器（普通 IP 多播数据报是要被多播路由器转发的）转发到其他网络，其 IP 数据报中的 TTL 被设置为 1，路由器收到该数据报后会丢弃该报文而不会被转发。

4-51 在 IGMP 中有了离开组报文和成员报告报文，是不是可以不需要路由器周期性发送成员查询报文了？请说明原因。

解答：不行。假设网络中某多播组仅有一个主机，但该主机突然意外关机了（如出现故障），也就是说不会再发送离开组报文了，多播路由器会认为有一个组成员一直在网络中。

4-52 请说明 IGMP 中组成员对多播路由器成员查询报文进行延迟响应的作用。

解答：为了减少不必要的重复应答（一个多播组只需有一个应答即可），采用了一种延迟响应策略。收到成员查询的主机，并不是立即响应，而是等待一段随机的时间（1~10 秒）后再进行响应。如果在这段时间内监听到同组其他成员发送的成员报告（本网络中所有该组

成员都能监听到）就取消响应行动。多播路由器如果长时间没有收到某个多播组的成员报告则将该多播组从维护的多播组列表中删除，即认为在本网络中没有该组的成员。

4-53 多播路由选择有哪两种基本的方法？

解答：多播路由选择的基本任务就是在多播路由器之间为每个多播组建立一个连接源（源主机连接的路由器）和所有成员路由器（拥有该组成员的路由器）的多播转发树。目前有两种基本的方法来构建多播转发树：

基于源树的多播路由选择。该方法为一个多播组内的每个源构建一棵多播转发树，该转发树通常由每个成员路由器到源的最短路径构成。

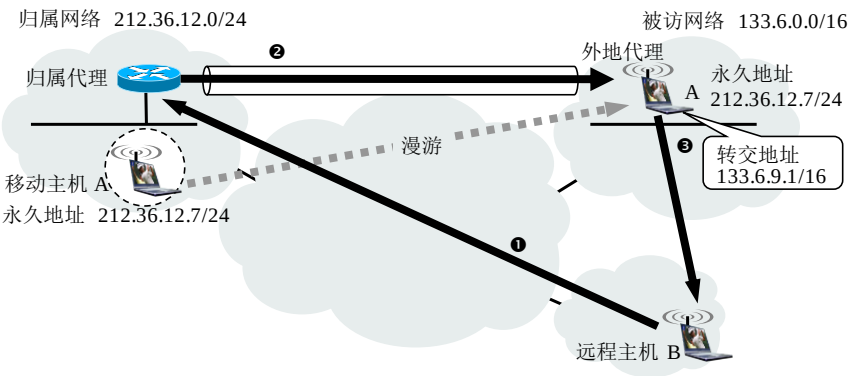
组共享树多播路由选择。该方法在每个多播组中指定一个中心路由器，以此中心路由器为根建立一棵连接所有成员路由器的多播转发树。多播组内的所有源共享这同一棵多播转发树，将多播分组通过单播 IP 隧道发送到中心路由器，再由中心路由器将多播分组在共享树上进行洪泛。

4-54 为什么说移动 IP 对于任何与移动主机进行通信的固定主机来说都是完全透明的？

解答：在移动 IP 中，固定主机发送数据报到移动主机以及固定主机接收移动主机发送的数据报都与正常情况完全一样，固定主机根本不需要知道是否在和移动主机通信，也不需要安装任何支持移动 IP 的软件和协议。

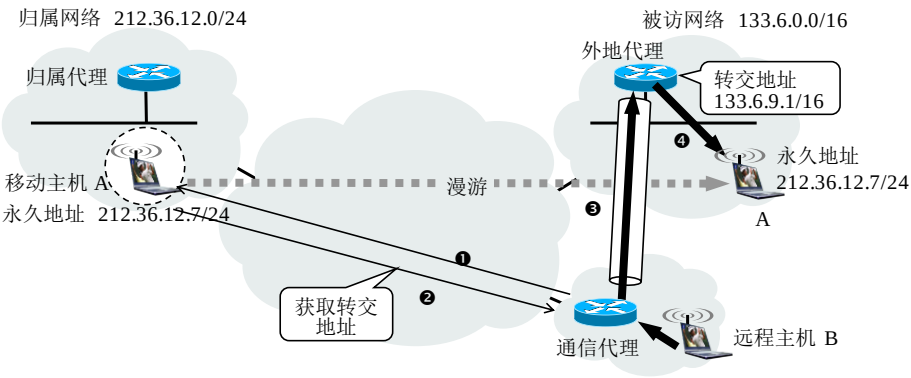
4-55 在移动 IP 中，若采用同址转交地址方式，请重画图 4-49。

解答：




4-56 在移动 IP 中，若采用直接路由方式而不是三角形间接路由，请重画图 4-49。

解答：




4-57 当前的移动 IP 标准包括哪三个主要部分？

解答：当前移动 IP 标准主要包括以下 3 个部分：

代理发现。定义归属代理或外部代理向移动主机通告其服务时，以及移动主机请求一个外部代理或归属代理的服务时所使用的协议。其中最重要的就是归属代理要将转交地址通告给移动主机。

信息注册。定义移动主机向外地代理注册或注销永久地址、归宿代理地址等信息，以及移动主机或外地代理向归宿代理注册或注销转交地址时所用的协议。

间接路由。定义了数据报由一个归属代理转发给移动主机的方式，包括转发数据报的规则、差错处理规则和几种不同的封装形式。

4-58 从 IPv4 过渡到 IPv6 的方法有哪些？

解答：主要有两种向 IPv6 过渡的策略，即使用双协议栈和使用隧道技术。

双协议栈是指在完全过渡到 IPv6 之前，使一部分主机（或路由器）装有两个协议栈，一个 IPv4 和一个 IPv6。因此双协议栈主机（或路由器）既能够和 IPv6 的系统通信，又能够和 IPv4 的系统进行通信。双协议栈主机在和 IPv6 主机通信时是采用 IPv6 地址，而和 IPv4 主机通信时就采用 IPv4 地址。

向 IPv6 过渡的另一种方法是隧道技术。在 IPv6 数据报要进入 IPv4 网络时，将 IPv6 数据报封装成为 IPv4 数据报，然后 IPv6 数据报就在 IPv4 网络的隧道中传输。当 IPv4 数据报离开 IPv4 网络中的隧道时，再将其数据部分（即原来的 IPv6 数据报）交给主机的 IPv6 协议栈。

4-59 在 IPv4 首部中有一个“协议”字段，但在 IPv6 的固定首部中却没有。这是为什么？

解答：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。

4-60 考虑图 4-56 中的 MPLS 网络，并假设路由器 $R_1$ 和 $R_2$ 也是 MPLS 标签交换路由器。若我们想执行这样的流量工程：从 $R_1$ 到 $N_1$ 的流量要经过 $R_3$ 和 $R_5$，而从 $R_2$ 到 $N_2$ 的流量则要经过 $R_3$、$R_4$ 和 $R_6$。请给出 $R_1$ 和 $R_2$ 中相应的 MPLS 转发表，并修改 $R_3$ 的转发表。

解答：答案不唯一

$R_1$ 路由表（入标签，出标签，目的地，出接口）：（－，x，$N_1$，0）

$R_2$ 路由表（入标签，出标签，目的地，出接口）：（－，y，$N_2$，0）

$R_3$ 路由表（入标签，出标签，目的地，出接口）：（x，10，$N_1$，0），（y，9，$N_2$，1）

## 第 5 章

5-1 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？

解答：从通信和信息处理的角度看，运输层向它上面的应用层提供端到端通信服务，它属于面向通信部分的最高层，同时也是用户功能中的最低层。当位于网络边缘部分的两台主机使用网络核心部分的功能进行端到端的通信时，只有主机的协议栈才有运输层，而网络核心部分中的路由器在转发分组时都只用到下三层的功能。

虽然网络层实现了主机到主机的逻辑通信，但严格地讲，通信的真正端点并不是主机而是主机中的进程。因此，运输层在网络层之上提供应用进程间的逻辑通信。

5-2 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无连接的？

解答：从网络层看是无连接的，但从运输层看是面向连接的。

5-3 接收方收到有差错的 UDP 用户数据报时应如何处理？

解答：丢弃且不通知发送方。

5-4 在“滑动窗口”概念中，“发送窗口”和“接收窗口”的作用是什么？如果接收方的接收能力不断地发生变化，则采取何种措施可以提高协议的效率。

解答：“发送窗口”作用是限制发送方连续发送数据的数量，即控制发送方发送数据的平均速率。“接收窗口”反映了接收方当前接收缓存的大小，即接收方接收能力的大小。当接收方的接收能力不断地发生变化时，可以将接收窗口的大小发送给发送方，调节发送方的发送速率，避免因发送方发送速率太大或太小而导致接收缓存的溢出或带宽的浪费，从而提高协议的效率。

5-5 简述 TCP 和 UDP 的主要区别。

解答：TCP 提供的是面向连接、可靠字的字节流服务，并且有流量控制和拥塞控制功能。UDP 提供的是无连接、不可靠的数据报服务，无流量控制和拥塞控制。

5-6 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。

5-7 如果因特网中的所有链路都提供可靠的传输服务，TCP 可靠传输服务将会是完全多余的吗？为什么？

解答：TCP 可靠传输服务不是多余的。因为在端到端的数据传输过程中并不是所有的差错都来自分组在链路上传输时的比特级差错，例如由于网络拥塞导致路由器的分组丢弃，路由器在转发分组时的故障等都会导致端到端的数据传输的差错，这些都不可能通过链路层的可靠数据传输得以解决，必须由端到端的运输层可靠数据传输服务来解决。

5-8 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。

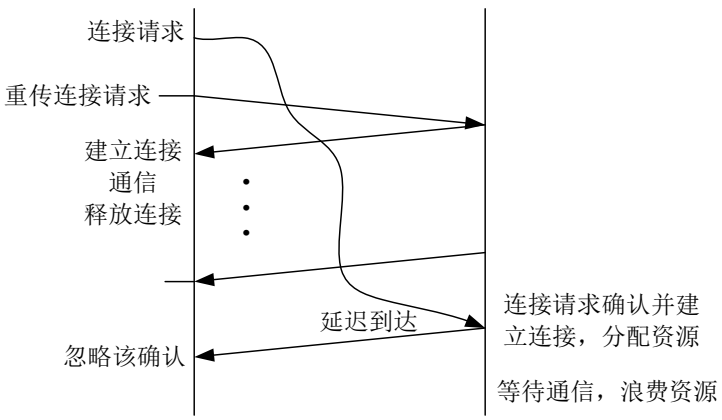
解答：假定 A 和 B 之间建立了 TCP 连接。如果 A 发送完数据在还没有接收到对方确认时就突然释放连接，则不能保证这些没有被确认的数据在传输中不会丢失。

如果 A 在收到 B 对所有发送数据的确认后释放连接，A 发送的数据不会丢失，可能 B 还在数据发送，这些数据 A 都无法正确收到。

TCP 的连接释放在两个方向都要发送连接释放请求和确认，保证数据不丢失。

5-9 试用具体例子说明为什么在运输连接建立时要使用三次联络。说明如不这样做可能会出现什么情况。

解答：这主要是为了防止已失效的连接请求报文段突然又传送到了 TCP 服务器，导致建立错误的连接而浪费资源，如图所示。




5-10 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？

解答：由于 IP 数据报的最大长度是 65535 字节，因此除去 IP 首部的 20 字节和 TCP 首部的 20 字节，一个 TCP 报文段的数据部分最多为 65495 字节。

如果用户要传送的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，则重复循环使用。

5-11 主机 A 和 B 使用 TCP 通信。在 A 接收到的报文段中，有这样连续的两个：ack = 120 和 ack = 100。这可能吗（前一个报文段确认的序号还大于后一个的）？试说明理由。

解答：一般不会，因为 TCP 的接收方采用的是累积确认，确认号不会倒退。但当出现失序时会有这种情况出现。设想 A 连续发送两个报文段：（seq = 92，DATA 共 8 字节）和（seq =100，DATA 共 20 字节），均正确到达 B。B 连续发送两个确认：(ack = 100) 和 (ack = 120)。但前者在网络中传送时经历了很大的时延，使得 A 先收到 B 后发送的确认。图 A-1 说明了这一情况。见图 A-1。

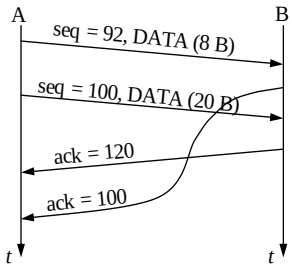



图 A-1　习题 5-11 的图

5-12　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。

解答：发送方还未超时重传就收到了接收方对更高序号的确认。

5-13　请简要比较 TCP 的可靠传输实现与 GBN 算法的主要异同。

解答：TCP 接收窗口大小不为 1，发送窗口和接收窗口大小动态变化，而 GBN 接收窗口为 1。

TCP 标准没有规定对不按序到达的数据应如何处理。通常是先临时存放在接收窗口中，等到字节流中所缺少的字节收到后，再按序交付上层的应用进程。

TCP 和 GBN 都是采用累积确认方式，但在发生超时，TCP 发送方仅对超时的分组重传，而 GBN 是重传窗口内所有已发送的分组。

TCP 的编号以字节为单位，而 GBN 以分组为单位。

因此 TCP 的算法介于 GBN 和 SR 之间。

5-14　在 5.3.3 节曾讲过，若收到的报文段无差错，只是未按序号，则 TCP 对此未作明确规定，而是让 TCP 的实现者自行确定。试讨论两种可能的方法的优劣：

(1) 把不按序的报文段丢弃；

(2) 先把不按序的报文段暂存于接收缓存内，待所缺序号的报文段收齐后再一起上交应用层。

解答：对于第一种方法，实现简单，接收方不需要很大的接收缓存，但由于所有不按序到达的报文段都被丢弃，这些报文段需要发送方进行重传，会浪费带宽。特别是在运输层，报文段不出现丢失也可能因 IP 报文独立路由而失序，而且由于端到端时延和时延抖动都比较大，超时时间设置的比较长，因此，失序报文段被接收方丢弃不仅浪费带宽而且重传会产生很大的时延。

对于第二种方法，只要在发送方超时前收到失序报文段的确认（接收方已收到所有迟到

的报文段，并发回确认），就可以避免失序报文段的重传。但协议更复杂，且需要比较大的接收缓存。

5-15 设 TCP 使用的最大窗口为 64 KB，即 64 × 1024 字节，而传输信道的带宽可认为是不受限制的。若报文段的平均往返时延为 20 ms，问所能得到的最大吞量是多少？

解答：$(64\times1024\times8)/(20\times10^{-3}) = 26.2\times10^{6}$ = 26.2 Mbit/s。

5-16 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 段链路程中有两段是卫星链路，有三段是广域网链路。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 250 ms。每一个广域网的范围为 1500 km，其传播时延可按 150 000 km/s 来计算。各数据链路速率为 48 kbit/s，帧长为 960 bit。

解答：每个广域网的传播时延 = (1500 km)/(150000 km/s) = 0.01 s = 10 ms

卫星链路传播时延 = 250 ms

每个结点的传输时延或发送时延 = (960 bit)/(48000 bit/s) = 0.02 s = 20 ms

因此，总的端到端单程时延为：10 ms × 3 + 250 ms × 2 + 20 ms × 5 = 630 ms。

5-17 重复上题，但假定其中的一个陆地上的广域网的传输时延为 150 ms。

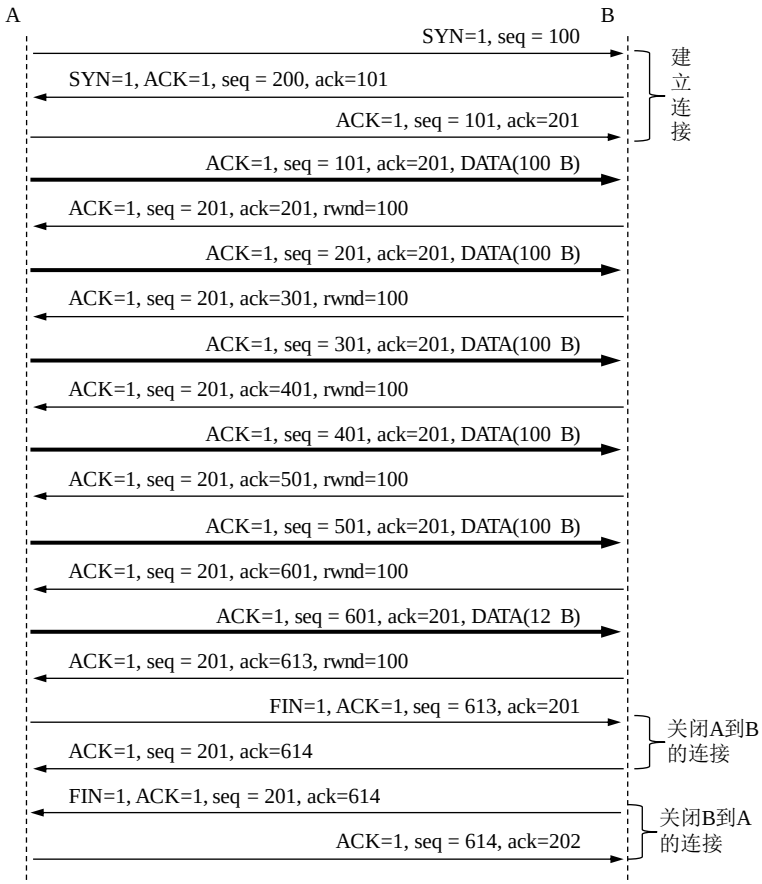
解答：760 ms。

5-18 TCP 接收方收到 3 个重复 ACK 就执行快速重传。为什么不在收到对报文段的第一个重复 ACK 后就快速重传？

答：当 TCP 接收方收到失序分组或重复分组时都会发送重复确认，而在运输层，失序是经常发生的，若对收到第一个冗余 ACK 后就快速重传，一旦两个报文段失序就会导致发送方立即快速重传，重传的分组又导致冗余 ACK（对重复分组的确认），又导致快速重传，不断这样下去。因此收到 3 个冗余 ACK 才认为丢失并进行快速重传，一是收到 3 个冗余 ACK 是因为丢失报文段的可能性比较大，二是即使没丢失也不会导致一直重传，很快能恢复正常。

5-19 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。再设发送方和接收方的起始序号分别选为 100 和 200，试画出类似于图 5-15 的工作示意图。从连接建立阶段到连接释放都要画上。

解答




5-20 在图 5-17 中所示的连接释放过程中，主机 B 能否先不发送 ack = u + 1 的确认？（因为后面要发送的连接释放报文段中仍有 ack = u + 1 这一信息）

解答：如果 B 也正要关闭连接，可以将对 A 的连接释放请求的确认和发给 A 的连接释放请求合并。但如果 B 并不马上关闭连接，则要及时对 A 的连接释放请求进行确认，否则 A 等待确认超时会重传连接释放请求。

5-21 在图 5-17 所示的连接释放过程中，主机 A 在发送完对 B 的连接释放请求报文段的确认后，为什么还要等待一段超时时间再彻底关闭连接？

解答：因为主机 A 的确认有可能丢失，这时 B 会重传 FIN 报文段。在这段超时时间内，若 A 又收到 B 重传的 FIN 报文段，A 需要再次进行确认。收到 A 的最后确认，B 才能最终将整个连接释放。主机 A 的 TCP 再向其应用进程报告，整个连接已经全部释放。

5-22 在图 5-18 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_SENT 到状态 SYN_RCVD 的变迁？

解答：当双方同时主动打开 TCP 连接，向对方发送连接请求（SYN）时，从状态 LISTEN 变为状态 SYN_SENT，然后收到对方的连接请求后，发送连接请求确认（SYN, ACK）从状

态 SYN_SENT 变为状态 SYN_RCVD。

5-23 是否 TCP 和 UDP 都需要计算往返时延 RTT？

解答：往返时延 RTT 只是对运输层的 TCP 协议才很重要，因为 TCP 要根据平均往返时延 RTT 的值来设置超时计时器的超时时间。

UDP 没有确认和重传机制，因此 RTT 对 UDP 没有什么意义。

5-24 在 TCP 的往返时延的估计中，你认为为什么 TCP 忽略对重传报文段的往返时延测量值 RTT 样本。

解答：因为分组丢失差错和过早超时都可能导致发送方重传分组，因此发送方无法确定接收到的确认是对原来发送的分组的确认还是对重传的分组进行确认。

若认为是对重传的分组进行确认，而实际上是过早超时，该分组是对原来发送的分组的确认，则可能测量值 SampleRTT 比实际值要小。

若认为是对原来发送的分组的确认，而实际上是对重传分组的确认，则测量值 SampleRTT 可能比实际值要大。

5-25 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？

解答：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会小于实际的往返时延，当再次发送报文段时，又会超时，若在超时重传后立即收到原报文段的确认，则重传时间会减小到接近于零。

5-26 某个应用进程使用运输层的用户数据报 UDP，然后继续向下交给 IP 层后，又封装成 IP 数据报。既然都是数据报，是否可以跳过 UDP 而直接交给 IP 层？哪些功能 UDP 提供了但 IP 没有提供？

解答：不能，IP 协议没有提供端口功能，IP 数据报只能找到目的主机而无法找到目的进程。

5-27 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？

解答：TCP 的流量控制和拥塞控制和可靠数据传输机制会导致比较大的分组时延抖动，而大的时延抖动会严重影响实时话音数据传输的质量。由于数据文件的传输需要可靠数据传输，因此在使用 UDP 在传送数据文件时需要应用程序自己实现可靠数据传输功能。

5-28 TCP 在进行拥塞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。

解答：有。一是信道误码导致中间结点将分组丢弃；二是路由错误导致分组在网络中兜圈子最后被路由器丢弃；三是中间路由器在接收了分组还没有转发出去时故障，导致分组丢

失。这些情况发生的概率都比较小。

5-29 一个应用程序用 UDP，到了 IP 层将数据报再划分为 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 个数据报片组装成为完整的数据报？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。

解答：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数据报。

5-30 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字段？

解答：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。如果没有首部长度字段，接收方就无法知道 TCP 报文段的数据从什么地方开始。TCP 首部中的首部长度字段也可以看成是数据偏移字段。而 UDP 首部长度是固定的，因此不需要首部长度字段。

5-31 一个 UDP 用户数据报的数据字段为 8192 字节。要使用以太网来传送。试问应当划分为几个数据报片？说明每一个数据报片的数据字段长度和片偏移字段的值。

解答：6 个。数据字段的长度：前 5 个是 1480 字节，最后一个是 800 字节。(注意要加上 UDP 首部的 8 字节)

片偏移字段的值分别是：0, 185, 370, 555, 740 和 925。

5-32 简述 TCP 流量控制和拥塞控制的不同。

解答：流量控制解决因发送方发送数据太快而导致接收方来不及接收使接收方缓存溢出的问题。流量控制的基本方法就接收方根据自己的接收能力控制发送方的发送速率。TCP 采用接收方控制发送方发送窗口大小的方法来实现在 TCP 连接上的流量控制。

拥塞控制就是防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。TCP 的发送方维持一个叫做拥塞窗口的状态变量。拥塞窗口的大小取决于网络的拥塞程度，当网络拥塞时减小拥塞窗口的大小，控制 TCP 发送方的发送速率。TCP 发送方的发送窗口大小取接收窗口和拥塞窗口的最小值。

5-33 在 TCP 的拥塞控制中，什么是慢开始、拥塞避免、快速重传和快速恢复算法？这里每一种算法各起什么作用？“加性增”和“乘性减”各用在什么情况下？

解答：慢开始就是当主机刚开始发送数据时完全不知到网络的拥塞情况，将拥塞窗口设为很小，当收到确认时，由小到大逐渐增大发送方的拥塞窗口数值。

在慢开始阶段发送速率以指数方式迅速增长，若持续以该速度增长发送速率必然导致网络很快进入拥塞状态。因此需要设置一个状态变量，即慢开始门限 ssthresh，当拥塞窗口大于该门限时，进入拥塞避免阶段，降低发送速率的增长速率（以线性方式增长），避免网络拥塞。

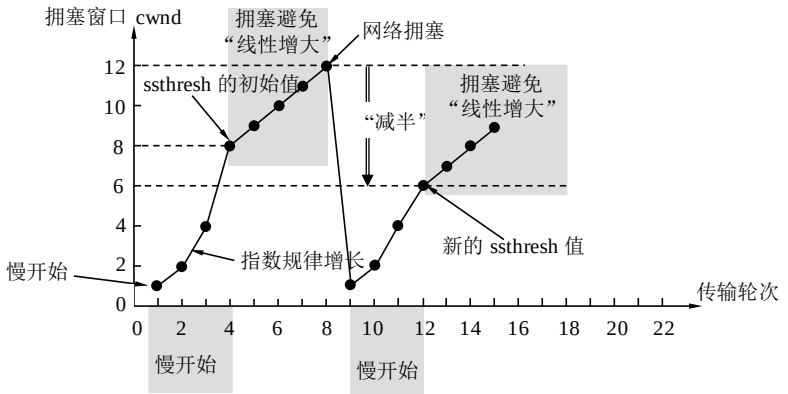
快速重传就是当发送方收到 3 个冗余确认时，就认为现在可能是网络出现了拥塞造成分组丢失，就立即重传确认号指示的报文段，而不必继续等待超时。

快速恢复就是，当发送方收到连续三个重复的 ACK 时，虽然有可能丢失了一些分组，但这连续的三个重复 ACK 同时又表明丢失分组以外的另外三个分组已经被接收方接收了。因此，与发生超时事件的情况不同，网络还有一定的分组交付能力，拥塞情况并不严重，直接执行拥塞避免算法。

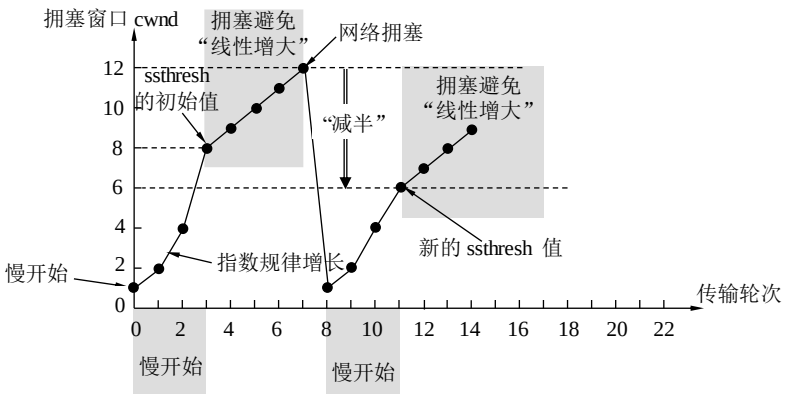
采用快速恢复算法的情况下，长时间的 TCP 连接在稳定的时候通常处于下面描述的重复状态。经过慢启动发送方迅速进入拥塞避免阶段，在该阶段，使拥塞窗口呈线性增长，即“加性增”，发送速率缓慢增长，以防止网络过早出现拥塞。当流量逐渐超过网络可用带宽时会出现拥塞，但由于发送速率增长缓慢，通常仅导致少量分组丢失。这种情况下发送方会收到 3 个重复 ACK 并将拥塞窗口减半，即“乘性减”，然后再继续执行“加性增”缓慢增长发送速率，如此重复下去。

5-34 TCP 使用慢开始和拥塞避免，设 TCP 的拥塞窗口阈值的初始值为 8（单位为 MSS）。从慢开始开始，当拥塞窗口上升到 12 时网络发生了超时。试画出每个往返时间 TCP 拥塞窗口的演变曲线图（横坐标单位为“轮次”，纵坐标为拥塞窗口大小）。说明拥塞窗口每一次变化的原因（画 15 个“轮次”）。

解答：拥塞窗口的变化：1, 2, 4, 8, 9, 10, 11, 12, 1, 2, 4, 6, 7, 8, 9。




(横坐标从 1 开始)




(横坐标从 0 开始，与书上一致)

5-35 通信信道带宽为 1 Gbit/s，端到端时延为 10 ms。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？

解答： 最大吞吐量：26.214 Mbit/s。信道利用率：2.6214%。(注意，该题并没有指出每个 TCP 报文段的大小，因此没有考虑每个报文段的发送时延)

5-36 为什么 TCP 拥塞控制中对发送方收到 3 个重复 ACK 和超时事件采用不同的处理方法？

解答：当发送方收到 3 个冗余 ACK 说明网络可能丢失了少量分组，但后续多个分组都被接收方收到了，因此网络拥塞并不严重，TCP 执行快速恢复算法，将拥塞窗口减半，直接进入拥塞避免阶段。而当超时事件发生时，说明发送的一连串分组都丢失了，网络拥塞比较严重，因此将拥塞窗口减少到最小，开始执行慢启动。

5-37 考虑图 5-18 中的例子，若将主机 C 到 $R_1$ 的链路带宽提高到 10000 Mbit/s，则所能达到的最大吞吐量大约会是多少？

解答：约 11 Mbit/s。

5-38 考虑图 5-23 的网络，路由器之间的链路带宽为 100 Mbit/s，假设主机到路由器的链路带宽无限。主机 A 到 C 的连接经过 $R_2$，B 到 D 的连接经过 $R_3$，C 到 A 的连接经过 $R_4$，D 到 B 的连接过 $R_1$。若无拥塞控制，各主机逐渐增大发送速率，会出现什么情况？

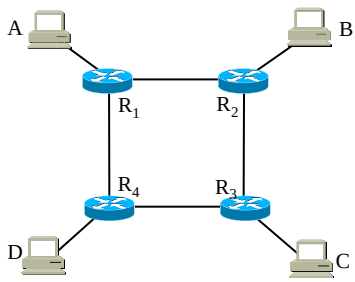



图 5-23 习题 5-38 的图

解答：随着各主机逐渐增大发送速率，网络总吞吐量逐渐增大到 200 Mbit/s（各主机发送速率为 50 Mbit/s），然后网络总吞吐量逐渐减少，当各主机发送速率增大到无穷大时，网络总吞吐量趋近于 0，即路由器之间的 4 条链路均满负荷，但各主机之间的分组传送均失败。

## 第 6 章

6-1 简述应用层协议定义的内容。

解答：(1)交换的报文类型，如请求报文和响应报文；

(2)各种报文类型的语法，如报文中的各个字段及其详细描述；

(3)字段的语义，即包含在字段中的信息的含义；

(4)进程何时，如何发送报文及对报文进行响应。

6-2 因特网的域名结构是怎样的？这样的结构有什么优点？

解答：因特网采用层次树状结构的命名方法，任何一个连接在因特网上的主机或路由器，都有一个唯一的层次结构的名字，即域名(domain name)。这里，“域”（domain)是名字空间中一个可被管理的划分。域还可以继续划分为子域，如二级域、三级域等等。域名的结构由若干个分量组成，各分量之间用点（请注意，是小数点的点）隔开。各分量分别代表不同级别的域名。每一级的域名都由英文字母和数字组成（不超过 63 个字符，并且不区分大小写字母），级别最低的域名写在最左边，而级别最高的顶级域名则写在最右边。

因特网域名的层次结构便于管理，等级的命名方法便于维护名字的唯一性。同时针对层次结构容易设计出高效的域名查询机制。

6-3 域名系统为什么不只使用一个域名服务器，而需要有很多服务器组成的分布式层次结构？

解答：集中方式有如下缺点：单点故障，可靠性差；流量集中导致周边网络拥塞；所有查询必须访问远程集中数据库；大量数据难以维护。而采用分布式层次结构可以解决这些问题。

6-4 域名系统的主要功能是什么？域名系统中的根服务器和权威服务器有何区别？权威服务器与管辖区有何关系？

解答：DNS 为其他各种网络应用提供一种核心服务，即名字服务，用来把计算机的名字转换为对应的 IP 地址。

名字空间相关信息（其中最重要的就是域名和 IP 地址的映射关系）必须保存在计算机中，供所有其他应用查询。显然不能将所有信息都存储在一台计算机中。DNS 的方法是将域名信息分布到叫做域名服务器的许多计算机上。DNS 将整个名字空间划分为许多区(zone)，每个区的域名信息由一个权威域名服务器负责管理。

根域名服务器是最高层次的域名服务器。根域名服务器并不直接管辖某个区的域名信息，但每个根域名服务器都知道所有的顶级域名服务器的域名及其 IP 地址。

6-5 举例说明域名解析的过程。域名服务器中的高速缓存的作用是什么？

解答：域名解析的过程例子：教材图 6-6。为了提高 DNS 查询效率，并减轻根域名服务器的负荷和减少因特网上的 DNS 查询报文数量，在域名服务器中广泛地使用了高速缓存（有时也称为高速缓存域名服务器）。高速缓存用来存放最近查询过的域名以及从何处获得域名映射信息的记录。

6-6 DNS 有哪两种域名解析方式，简述这两种方式区别和特点。

解答：递归查询: 被请求的域名服务器负责域名的解析，当被请求者自己无法解析时，代替请求者查询，服务器负担重。

迭代查询: 被请求的服务器不能解析时仅返回另一个服务器的域名和地址，让请求者自己重新查询，即回答“我不知道这个名字, 请问这个服务器吧!”。请求这负担重。

6-7 为什么通常从请求主机到本地域名服务器的查询采用的是递归查询，而其余的查询采用迭代查询？

解答：从理论上讲，任何 DNS 查询既可以采用递归查询也可以采用迭代查询。但由于递归查询对于被查询的域名服务器负担太大，而采用迭代查询对请求主机产生的负担太大。通常从请求主机到本地域名服务器的查询是递归查询，而其余的查询是迭代查询。

6-8 对同一个域名向 DNS 服务器发出好几次的 DNS 请求报文后，每一次得到 IP 地址都不一样。这可能吗？

解答：可能。DNS 允许用同一个主机名对应一个 IP 地址集合。DNS 服务器收到该主机名的解析请求时，随机或循环返回地址集合中的一个地址。一些热门网站，可以利用该服务将网站复制到多个服务器上，这些服务器公用同一个域名，从而实现在这些服务器上的负载分配。

6-9 根据所学原理，你认为部署一个 DNS 权威域名服务器必须做哪些基本配置？

解答：必须做 3 种基本配置，具体如下：

（1）该服务器上配置至少一个根服务器的地址。大部分 DNS 服务器程序在其配置中提供了所有 13 个根服务器的完整列表。

（2）该服务器中要配置所管理的管理范围，及维护的域名与 IP 地址的映射信息。

（3）要在上级域名服务器中将相关子域委托给该服务器管理，并记录该服务器的地址。

6-10 解释以下名词。各英文缩写词的原文是什么？

WWW、URL、HTTP、HTML、浏览器、超文本、超媒体、超链、页面、动态文档、活动文档。

解答：

WWW (World Wide Web)是万维网的英文缩写。万维网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，现在经常只用一个英文字 Web 来表示万维网。万维网利用网页之间的链接（或称为超链接，即到另一个网页的指针）将不同网站的网页链接成一张逻辑上的信息网，从而用户可以方便地从因特网上的一个站点访问另一个站点，主动地按需获取丰富的信息。

URL (Uniform Resource Locator)是统一资源定位符的英文缩写。万维网使用 URL 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 (HyperText Transfer Protocol) 是超文本传送协议的英文缩写。HTTP 是浏览器与万维网服务器之间的交互所遵守的协议。HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。

HTML (HyperText Markup Language)是超文本标记语言的英文缩写。使得万维网页面的制作者可以很方便地用超链接从本页面的某处链接到因特网上的任何一个万万维网页面，并且制作出来页面能够在任何浏览器的窗口中显示。

浏览器是在万维网客户程序，用来向 Web 服务器请求页面，并向用户显示从 Web 服务器请求的页面。

超文本由多个信息源链接成，而这些信息源的数目实际上是不受限制的。利用一个链接可使用户找到另一个文档，而这又可链接到其他的文档（依次类推）。这些文档可以位于世界上任何一个接在因特网上的超文本系统中。超文本是万维网的基础。

超媒体与超文本的区别是文档内容不同。超文本文档仅包含文本信息，而超媒体文档还包含其他多媒体对象，如图形、图像、声音、动画，甚至活动视频图像。

超链就是超文本的链接，超链是隐藏在页面文字或图片后面的 URL，该 URL 指向另一个页面或文件，通常与超链关联文字是用特殊方式显示的（例如用不同的颜色，或添加了下划线），而当我们将鼠标移动到这些地方时，鼠标的箭头就变成了一只手的形状。

页面就是显示在浏览器中的万维网文档，也称为网页。

动态文档是指文档的内容是在浏览器访问万维网服务器时才由应用程序动态创建的。

活动文档是一种能提供页面连续变化而无需不断请求服务器的技术。实际上一个活动文档就是一段程序或嵌入了程序脚本的 HTML 文档。活动文档中的程序可以在浏览器运行，从而产生页面的变化（例如弹出下拉菜单或显示动画等）。

6-11 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指向一个无效的计算机名字。这时浏览器将向用户报告什么？

解答：域名无法解析。

6-12 假定在同一 Web 服务器上的某 HTML 文件引用了 3 个非常小的对象（例如图片）。忽略发送时间，往返时延为 RTT，不考虑连接释放时间，在下列各种情况下将该页面完整接收下来需要多长时间？

(1) 采用非并行 TCP 连接的 HTTP 非持续连接方式；

(2) 采用并行 TCP 连接的 HTTP 非持续连接方式；

(3) 采用 HTTP 持续连接非流水线方式；

(4) 采用 HTTP 持续连接流水线方式。

解答：(1)8RTT; (2)4RTT; (3)5RTT; (4)3RTT。

6-13 考虑一个电子商务网站需要保留每一个客户的购买记录。描述如何使用 Cookie 机制来完成该功能。

解答：步骤如下。

（1）用户第 1 次访问电子商务网站时，服务器在 HTTP 响应报文中的 cookie 首部行中加入一个新产生的用户 ID，并在服务器的后端数据库中建立相应记录。

（2）在用户主机中产生 Cookie 文件，由用户浏览器管理。

（3）用户下一次访问时，浏览器在其 HTTP 请求报文中的 Cookie 首部行中引用服务器所分配的用户 ID，用户的购买记录会被记录在后台数据库中。

6-14 简述 Web 缓存的作用和工作原理。

解答：Web 缓存器可以减少对客户机请求的响应时间，减小一个机构内部网络与因特网接入链路的通信量，作为代理服务器的另一个作用就是可以用来隔离内外网络。用户配置浏

览器: 通过 Web 缓存访问 Web，浏览器发送所有 HTTP 请求到 Web 缓存，若对象在缓存中: 缓存返回对象，否则每个缓存器从原始服务器请求对象，存储在本地，然后返回一个复本给客户机。

6-15 请进行一个实验：把你的计算机与网络断开，用脱机方式访问几个你经常访问的 Web 网站，看能不能够正常显示这些页面。在你的计算机中找到你浏览器的高速缓存的文件夹，看看里面存放了多少个页面？

解答：略，IE 默认的缓存位置是 C:\Documents and Settings\用户名\Local Settings\Temporary Internet Files\

6-16 试比较万维网静态文档、动态文档和活动文档的区别。

解答：静态文档是指该文档创作完毕后就存放在万维网服务器中，在被用户浏览的过程中，内容不会改变。由于这种文档的内容不会改变，因此用户对静态文档的每次读取所得到的返回结果都是相同的。在万维网发展的早期，所有的文档都是静态的。然而，随着万维网技术的发展越来越多的网页都是动态生成的，即动态文档。

动态文档是指文档的内容是在浏览器访问万维网服务器时才由应用程序动态创建的，其内容通常来源于数据库并根据客户请求报文中的数据动态生成的。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，并把控制转移到此应用程序。接着，该应用程序对浏览器发来的数据进行处理，并输出 HTTP 格式的文档，万维网服务器把应用程序的输出作为对浏览器的响应。

活动文档是一种能提供页面连续变化而无需不断请求服务器的技术。实际上一个活动文档就是一段程序或嵌入了程序脚本的 HTML 文档。活动文档中的程序可以在浏览器运行，从而产生页面的变化（例如弹出下拉菜单或显示动画等）。由于所有的更新工作都由浏览器自己在本地完成，无需向服务器不断请求页面，因此可以提高应用的响应速度，并对网络带宽的要求也不会太高。对于万维网服务器，活动文档和静态文档没有什么区别，活动文档仅在浏览器一端“活动”。活动文档有时也叫做客户端动态文档。

6-17 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？

解答：电子邮件系统的三个主要组成构件：用户代理、邮件服务器，以及发送和接收电子邮件所需的协议。用户代理 UA 就是用户与电子邮件系统的接口，又称为电子邮件客户端软件。用户代理使用户能够通过一个很友好的接口（目前主要是用窗口界面）来撰写、发送、接收和阅读邮件。现在可供大家选择的用户代理有很多种。没有 UA 用户就不能处理和发送邮件。

6-18 电子邮件的信封和内容在邮件的传送过程中起什么作用？

解答：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才能见到邮件的内容。在邮件的信封上，最重要的就是收件人的电子邮件地址（或电子信箱地址），没有信封就不能将邮件正确地发送到

收件人的邮件。

6-19 电子邮件的地址格式是怎样的？请说明各部分的意思。

解答：电子邮件的地址格式为：收件人邮箱名@邮箱所在服务器域名。符号“@”应读作“at”，表示“在”的意思。用户名是收件人自己定义的字符串标识符，作为收件人在这个域名中的邮箱名。标志收件人邮箱名的字符串在邮箱所在的邮件服务器中必须是唯一的，由于一个邮箱所在邮件服务器的域名在因特网中是唯一的，因此每一个用户的电子邮件地址在因特网中也是唯一的。

6-20 试简述 SMTP 通信的三个阶段的过程。

解答：

1. 连接建立。发件人的邮件送到发送方邮件服务器的邮件缓存后，SMTP 客户就每隔一定时间对邮件缓存扫描一次。如发现有邮件，就使用 SMTP 的熟知端口号码(25)与接收方邮件服务器的 SMTP 服务器建立 TCP 连接。

2. 邮件传送。邮件的传送从 MAIL 命令开始。MAIL 命令后面有发件人的地址。下面跟着一个或多个 RCPT 命令，取决于把同一个邮件发送给一个或多个收件人。RCPT 命令的作用就是：先弄清接收方系统是否已做好接收邮件的准备，然后才发送邮件。再下面就是 DATA 命令，表示要开始传送邮件的内容了。

3. 连接释放。邮件发送完毕后，SMTP 客户应发送 QUIT 命令。SMTP 若同意释放 TCP 连接，邮件传送的全部过程即结束。

6-21 试述邮局协议 POP 的工作过程。在电子邮件中，为什么必须使用 POP 和 SMTP 这两个协议？IMAP 与 POP 有何区别？

解答：由于 SMTP 是一种“推”协议，不能用来完成读取邮件这样“拉”的任务，发送邮件是客户主动将邮件“推送”到邮件服务器的过程，而接收邮件是客户主动从邮件服务器“拉取”邮件的过程。因此 SMTP 协议用来发送电子邮件，而 POP 协议用来读取电子邮件。

邮局协议 POP 是一个非常简单、但功能有限的邮件读取协议。当用户需要从邮件服务器的邮箱中下载电子邮件时，客户就开始读取邮件。客户（用户代理）在 TCP 端口 110 打开到服务器的连接。它然后发送用户名和口令，访问邮箱。用户可以列出邮箱中的邮件清单，并逐个读取邮件文件。

POP3 有两种工作方式：下载并删除方式和下载并保留方式。下载并删除方式就是在每一次读取邮件后就把邮箱中的这个邮件删除。保存方式就是在读取邮件后仍然在邮箱中保存这个邮件。删除方式通常用在用户使用固定计算机工作的情况，用户在本地计算机中保存和管理所收到的邮件。下载并保留方式允许在不同的计算机上多次读取同一邮件。

虽然 POP3 提供了下载并保留方式，但它不允许用户在服务器上管理他的邮件，例如创建文件夹，对邮件进行分类管理等。因此 POP3 用户代理采用的主要模式是将所有邮件下载到本地进行管理。这种方式对于经常使用不同计算机上网的移动用户来说是非常不方便的。

另一个读取邮件的协议是因特网报文存取协议 IMAP。在使用 IMAP 时，在用户的 PC 上运行 IMAP 客户程序，然后与接收方的邮件服务器上的 IMAP 服务器程序建立 TCP 连接。

用户在自己的 PC 上就可以操纵邮件服务器的邮箱，就像在本地操纵一样，因此 IMAP 是一个联机协议。用户可以根据需要为自己的邮箱创建便于分类管理的层次式的邮箱文件夹，并且能够将存放的邮件从某一个文件夹中移动到另一个文件夹中。用户也可按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。这样就省去了用户 PC 硬盘上的大量存储空间。

IMAP 最大的好处就是用户可以在不同的地方使用不同的计算机（例如，使用办公室的计算机、或家中的计算机，或在外地使用笔记本计算机）随时上网阅读和处理自己的邮件。

6-22 MIME 与 SMTP 的关系是怎样的？什么是 quoted-printable 编码和 base64 编码？

解答：由于 SMTP 限于传送 7 位的 ASCII 码，不能传送可执行文件或其他的二进制对象。为解决 SMTP 传送非 ASCII 码文本的问题，提出了通用因特网邮件扩充 MIME。MIME 并没有改动或取代 SMTP，只是一个辅助协议。MIME 在发送方把非 ASCII 码数据转换为 ASCII 码数据，交给 SMTP 传送。在接收方再把收到的数据转换为原来的非 ASCII 码数据。

quoted-printable 编码适用于当所传送的数据中只有少量的非 ASCII 码，例如汉字。这种编码方法的要点就是对于所有可打印的 ASCII 码，除特殊字符等号“=”外，都不改变。等号“=”和不可打印的 ASCII 码以及非 ASCII 码的数据的编码方法是：先将每个字节的二进制代码用两个十六进制数字表示，然后在前面再加上一个等号“=”。

对于任意的二进制文件，可用 base64 编码。这种编码方法是先将二进制代码划分为一个个 24 位长的单元，然后将每一个 24 位单元划分为 4 个 6 位组。每一个 6 位组按以下方法转换成 ASCII 码。6 位的二进制代码共有 64 种不同的值，从 0 到 63。用 A 表示 0，用 B 表示 1，等等。26 个大写字母排列完毕后，接下去再排 26 个小写字母，再后面是 10 个数字，最后用+表示 62，而用/表示 63。再用两个连在一起的等号==和一个等号=分别表示最后一组只有 8 位或 16 位的代码。解码时对回车和换行都忽略，因此它们可在编码后的字符串中的任何地方插入。

6-23 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？

解答：发送编码后的数据 3072×32/24=4095 字节，插入回车符换行符 104 个，因此一共发送了 4200 字节。

6-24 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？

解答：电子邮件系统虽然使用 TCP 传送邮件，但并不是在发件者和收件者之间直接使用 TCP 传送邮件，而是通过用户代理发送到发件方邮件服务器，然后发件方邮件服务器发送到收件方邮件服务器，若邮件服务器出现故障则可能导致我们收不到邮件。

6-25 当我们用浏览器访问某个网站时，如果输入的网站地址错误，浏览器会立即提示出现了错误，为什么我们在发送电子邮件时，当收件人地址写错时并不能立即得到错误信息呢？

解答：因为用户代理是先将邮件发送给邮件服务器，邮件服务器再在合适的时候将邮件发送给收件人所在的邮件服务器。当我们用用户代理发送邮件时邮件服务器并不处理邮件中的地址，也发现不了该错误，若邮件地址中的收件人邮箱所在邮件服务器域名错误，在发送方邮件服务器发送该邮件时会发现该错误，若邮件地址中是收件人邮箱名错误则要等该邮件发送到收件人邮箱所在邮件服务器时才可能发送该错误。

6-26 用户经常需要在不同的地方和不同的主机上接收和发送电子邮件，使用哪种邮件访问方式比较合适？

解答：IMAP 或使用基于万维网的电子邮件。

6-27 文件传送协议 FTP 的主要工作过程是怎样的？主进程和从属进程各起什么作用？

解答：FTP 基于客户/服务器体系结构。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。

主进程的工作步骤如下：

(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。

6-28 某用户利用 FTP 从远程主机下载了 3 个文件，在 FTP 客户机和 FTP 服务器之间至少要建立最少次 TCP 连接？为什么？

解答：4 个 TCP 连接。一次控制连接，3 次数据连接。

6-29 假设在因特网上有一台 FTP 服务器，其域名为 ftp.jfjlgdx.edu.cn，IP 地址为 212.56.121.23，FTP 服务器进程在默认端口守候并支持匿名访问（用户名：anonymous，口令：guest）。如果某个用户直接用服务器域名访问该 FTP 服务器，并从该服务器下载文件 File1 和 File2，请给出 FTP 客户进程与 FTP 服务器进程之间的交互过程。

解答：交互过程大致如下。

（1）首先要完成对该服务器域名 ftp.jfjlgdx.edu.cn 的解析，最终获得该服务器的 IP 地址 212.56.121.23。

（2）FTP 的客户进程与服务器进程之间使用 TCP 建立起一条控制连接，并经过它传送包括用户名和密码在内的各种 FTP 命令。

（3）控制连接建立之后，客户进程和服务器进程之间使用 TCP 建立两次数据连接，分别完成文件 File1 和 File2 的传输。

（4）当文件 File1 和 File2 传输完成之后，客户进程与服务器进程分别释放数据连接和控制连接。

6-30 如果一台计算机要接入到因特网，那么它必须配置哪些协议参数？DHCP 协议的作用是什么？

解答：一台连接到因特网的计算机通常需要配置以下参数：

(1) IP 地址。

(2) 子网掩码。

(3) 默认路由器的 IP 地址。

(4) 域名服务器的 IP 地址。

动态主机配置协议 DHCP (Dynamic Host Configuration Protocol)提供了一种机制，称为即插即用连网(plug-and-play networking)。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。

6-31 简述 DHCP 的工作过程。为什么要使用广播？

答：DHCP 客户广播 DHCP 服务器发现报文。DHCP 服务器应答 DHCP 提供报文。客户机发送 DHCP 请求报文。服务器应答 DHCP 确认报文。

使用广播发送 DHCP 服务器发现报文是因为客户不知道服务器的 IP 地址，但又想与之通信。

6-32 一台服务器采用 P2P 文件分发方式把一个大文件（长度为 $L$）分发给 $n$ 台客户机。假设文件传输的瓶颈是各主机的上行速率 $R$，并且每个对等方只能在接收完整个文件后才能向其它对等方转发。请计算文件分发到所有对等方的最短时间。

解答：$(L/R)\lceil \log_2(n+1) \rceil$

6-33 重新考虑上题文件分发任务，但可以将这个非常大的文件划分为一个个非常小的数据块进行分发，即一个对等方在下载完一个数据块后就能向其他对等方转发，并同时可下载其它数据块。不考虑分块增加的控制信息，试计算整个大文件分发到所有对等方的最短时间。

解答：$L/R$

6-34 在 P2P 对等方中搜索文件的方式主要有哪几种？简述各自的优缺点。

答：集中式目录、洪泛查询和 DHT。

集中式目录方式的优点是简单高效；缺点主要是单点故障、性能瓶颈。

洪泛查询方式的优点是完全分布无单点故障的问题，但缺点是查询流量大，可扩展性差，洪泛查询范围受限。

DHT 的优点是对精确查询高效、可靠、可扩展性好，但缺点是结构维护机制比较复杂，当结点频繁加入或退出会导致较高的维护代价，难以实现基于内容的模糊查询。

6-35 考虑一个 5 位 ID 空间的 Chord 覆盖网络，该覆盖网络有结点 1, 4, 7, 12, 15, 20, 27。假设结点 1 要查找对象 16，请写出查找步骤，并给出相关结点的索引表。

解答：查找步骤：1->12->15->20

结点 1 的索引表：4, 4, 7, 12, 20；结点 12 的索引表：15, 15, 20, 20, 1；

结点 15 的索引表：20, 20, 20, 27, 1；结点 20 的索引表：27, 27, 27, 1, 4；

6-36 常用的多媒体应用（流式存储音频/视频、流式实况音频/视频和实时交互音频/视频）都各有何特点？

解答：

流式存储音频/视频是一些经过压缩并存储在服务器中的文件，客户端可以通过因特网边下载边播放这些文件，也就是我们有时所说的音频/视频点播。所谓“流式”是指可以在下载文件的同时连续播放该文件。流式音频/视频又称为流媒体。

流式实况音频/视频（又称为音频/视频直播）类似于传统的广播电台和电视台播放的音频和视频节目，区别在于它们是通过因特网来传输的。这样的应用主要包括因特网广播电台和因特网电视。

实时交互音频/视频这类应用允许人们相互之间使用音频/视频进行实时的交互。典型的实例是因特网电话和因特网视频会议。

6-37 试简述 RTP 协议和 SIP 协议的要点。

解答：实时传输协议 RTP (Real-time Transport Protocol)用于传输多种格式的多媒体数据，RTP 协议分组封装在 UDP 报文中进行传输，并提供序号、时间戳等机制，在 UDP 之上为实时多媒体网络应用提供端到端的传输服务。

会话发起协议 SIP (Session Initiation Protocol)是一个由 IETF 制定的一套较为简单且实用的实时交互协议，能够用来定位用户、建立、管理和终止多媒体会话（呼叫），支持双方、多方或多播会话，但并不强制使用特定的编解码器和多媒体传输协议。

6-38 在万维网中寻找两个流式存储音频或视频网站。用 Wireshark 软件分析：

(1) 该站点是否使用了元文件?

(2) 音频/视频是利用 UDP 还是 TCP 进行传输的？

(3) 是否使用了 RTP？

(4) 是否使用了 RTSP？

解答：略

6-39 TCP 接收缓冲区和媒体播放器的播放缓冲区在作用上有什么区别？

解答：TCP 接收缓冲区用来存放已正确接收但接收方还来不及读取的数据，或者未按序到达，还不能提交给上层应用的数据。主要是用来匹配收发双方的速度的。

而媒体播放器的播放缓冲区是用来延迟播放的，将不等时到达的数据通过缓存后再以恒定速率按顺序将这些分组的数据进行播放。

6-40 RTP 协议能否为应用层提供可靠传输服务？请说明理由。

解答：不能。RTP 底层采用提供不可靠传输服务的 UDP，并且 RTP 本身也没有确认和

差错恢复机制。

6-41 在 RTP 分组首部中为什么要使用序号、时间戳？

解答：接收方可以通过序号检测是否丢失了分组，然后通过丢失分组恢复技术重构丢失的数据，以实现数据播放的连续性。要注意的是，RTP 本身并不提供修复数据丢失的任何措施，而只是把数据丢失的信息提供给媒体应用，并由应用来决定如何处理。

接收方使用时间戳来消除网络中引入的分组时延抖动，使接收方能够以恒定速率播放媒体。时间戳还可用于视频应用中声音和图像的同步。

6-42 试比较 CDN 与 Web 缓存的相似之处和区别。

解答：都是将内容复制到与用户距离较近的地方，从而避免了大量重复数据的远程传输，大大改善整个系统的传输时延和网络流量。但 CDN 是主动将内容推送到用户附近，而 Web 缓存是其他用户访问时缓存到用户附近。另外，在 CDN 中，用户是先直接访问原始服务器，然后被重定向到副本结点；而使用 Web 缓存时，用户是先访问缓存，如果缓存没有，缓存再到原始服务器获取内容。

6-43 请说明 IP 多播和应用层多播的区别。为什么目前流式实况频/视频应用多采用应用层多播技术来实现？

解答：IP 多播是通过多播路由器实现分组的复制和转发，而应用层多播的基本思想是把对多播数据的路由选择、复制和转发任务，交给位于网络边缘的多播组成员主机来完成，而不是由网络核心的路由器来直接处理多播数据。成员主机之间的数据传输依然采用的是 IP 单播。IP 多播的效率要比 P2P 应用层多播的效率要高，但广泛应用 IP 多播的前提是所有路由器都要具有复杂的 IP 多播功能，这势必增加路由器的负担和实现的复杂性，因此 IP 多播并没有得到很好发展和广泛使用。事实上把过于复杂的功能引入到网络层，就违反了因特网设计的“端到端原则”，而应用层多播正是将复杂的功能放在了位于网络边缘的端系统上。

6-44 在 SIP 协议中，SIP 注册服务器的作用是什么？

解答：由于在 SIP 中，用户呼叫对方的 SIP 地址不一定是 IP 地址，但实际通信是需要对方的 IP 地址。SIP 的注册服务器和 DNS 服务器非常类似：DNS 服务器把主机名解析成 IP 地址，而 SIP 注册服务器把 SIP 地址转换成 IP 地址。用户在任何时候使用 SIP 时，都应向注册服务器报告现在使用的 IP 地址。当主叫方需要和该被叫方通信时，通过注册服务器查找注册的被叫方的 IP 地址。

6-45 考察 6.10.2 节中 TCP 服务器代码的第 28、29 行。如果客户端发送一个比较长的字符串（例如 5000 字节），如何修改这两行代码才能正确接收完客户端发送的字符串，并说明原因。

解答：扩大 buf，并循环调用 recv 进行接收数据直到返回值小于等于 0，代码略。注意：TCP 的发送方由于流量控制和拥塞控制或将数据分多次发送过来，同时 5000 字节也大于以太网的最大帧长了。

6-46 判断正误：

(1) 在浏览器和 Web 服务器之间使用流水线方式的持久连接的话，一个 TCP 报文段可能携带两个不同的 HTTP 服务请求报文。

(2) 高质量视频传输属于能容忍数据丢失的网络应用。

(3) 假设用户请求由某些文本和两幅图片组成的 Web 页面（不使用内含图像文档）。对于这个页面，浏览器将会发送一个请求报文并接收三个响应报文。

(4) 由于 P2P 文件共享系统采用的是对等体系结构，因此在该系统中的一次通信会话中不存在客户机进程和服务器进程的概念。

(5) 全球目前有十几个根域名服务器，世界上任何一个联网计算机的域名都可以在其中至少一个根域名服务器的数据库中直接查询得到。

(6) 两个不同的 Web 页面（例如，www.mit.edu/research.html 及 www.mit.edu/students.html）可能通过同一个持久连接发送。

解答：(1) √ (2) √ (3)× (4)× (5)× (6) √

## 第 7 章

7-1 计算机网络中的安全威胁都有哪些？需要哪些安全服务？

解答：

计算机网络所面临的安全威胁主要来自两大类攻击，即被动攻击和主动攻击。这两类攻击中四种最基本的形式是：

(1) 截获(interception)　攻击者从网络上窃听他人的通信内容。

(2) 中断(interruption)　攻击者有意中断他人在网络上的通信。

(2) 篡改(modification)　攻击者故意篡改网络上传送的报文。

(4) 伪造(fabrication)　攻击者伪造信息在网络上传送。

除此之外，在被动攻击中，还有通信量分析；在主动攻击中还有重放攻击、拒绝服务攻击、恶意程序攻击等。

计算机网络需要的安全服务包括：机密性、报文完整性、不可否认性、实体鉴别、访问控制、可用性。

7-2 请说明授权(authorization)与鉴别(authentication)的区别。

解答：鉴别与授权(authorization)是不同的概念。授权涉及到的问题是：实体所进行的行为是否被允许（如是否可以对某文件进行读或写等等）。

7-3 对称密钥密码体制与公钥密码体制的特点各如何？各有何优缺点？

解答：对称密钥密码体制是一种加密密钥与解密密钥相同的密码体制。在对称钥密系统中，两个参与者要共享同一个秘密密钥，这给密钥的管理和更换都带来了极大的不便，通常需要使用复杂的密钥分发中心 KDC (Key Distribution Center)来解决该问题。然而采用公钥密

码体制可以比较容易地解决这个问题。

公钥密码体制使用不同的加密密钥与解密密钥，加密密钥（即公钥）PK 是公开信息，而解密密钥（即私钥）SK 是需要保密的，因此私钥也叫做秘密密钥。由于加密密钥不能用来解密，并且从加密密钥不能推导出解密密钥，因此加密密钥可以公开。例如，参与者 A 可以在报纸上公布自己的加密密钥（即公钥），而解密密钥（即私钥）自己秘密保存。任何参与者都可以获得该公钥并用来加密发送给参与者 A 的信息，而该信息只能由 A 解密。可见采用公钥密码体制更易解决密钥分发的问题。

公钥密码体制有许多很好的特性，使得它不仅可以用于加密，还可以很方便地用于鉴别和数字签名。但是，公钥密码算法比对称密码算法要慢好几个数量级。因此，对称密码被用于绝大部分加密，而公钥密码则通常用于会话密钥的建立。

7-4 考虑 $n$ 个用户两两间的秘密通信问题。如果使用对称密钥密码体制，需要多少密钥？若使用公钥密码体制，则需要多少对密钥？

解答：使用对称密钥密码体制，需要的密钥数是 $n(n-1)/2$ 个。使用公钥密码体制，则需要 n 对密钥。

7-5 你能设计出一个简单的对称密钥加密算法吗？请大致评估一下你的加密算法的强度。

解答：略

7-6 在对称密钥系统中，通信双方要共享同一秘密密钥，需要通过安全通道分发密钥。而在公钥系统中，公钥无需保密，是否就不存在密钥分发的问题？试举一例说明原因。

解答：不是，设想用户 A 要欺骗用户 B。A 可以向 B 发送一份伪造是 C 发送的报文。A 用自己的私钥进行数字签名，并附上 A 自己的公钥，谎称这公钥是 C 的。B 如何知道这个公钥不是 C 的呢？因此，在公钥系统中也存在密钥分发的问题，通常需要有一个值得信赖的机构来将公钥与其对应的实体（人或机器）进行绑定(binding)，这样的机构就叫作认证中心 CA (Certification Authority)。

7-7 比较对称密钥密码体制与公钥密码体制中密钥分发的异同。

解答：其共同点是都需要一个可信的机构。目前常用的对称密钥分发方式是设立密钥分发中心 KDC。KDC 是一个大家都信任的机构，其任务就是给需要进行秘密通信的用户临时分发一个会话密钥。而在公钥系统中，通常需要有一个值得信赖的机构即认证中心 CA (Certification Authority)来将公钥与其对应的实体（人或机器）进行绑定(binding)。

7-8 为什么需要进行报文鉴别？报文的保密性与完整性有何区别？什么是 MD5？

解答：有时，通信双方并不关心通信的内容是否会被人窃听，而只关心通信的内容是否被人篡改或伪造，这就需要进行报文鉴别，既鉴别报文的真伪。

报文的机密性是确保报文中的信息不会泄漏给非授权用户。而报文完整性是确保报文中的信息不被非授权用户篡改或伪造。MD5 是一种报文摘要算法，用来进行报文鉴别。

7-9 为什么报文鉴别技术中要使用报文摘要？什么报文摘要要使用密码散列函数？使用普通散列函数会有什么问题？

解答：使用加密就可达到报文鉴别的目的，因为伪造的报文解密后不能得到可理解的内容。但对于不需要保密，而只需要报文鉴别的网络应用，对整个报文的加密和解密，会使计算机增加很多不必要的负担（加密和解密要花费相当多的 CPU 时间）。更有效的方法是使用报文摘要 MD (Message Digest)将可长的可变长报文计算得到较短的固定长度的报文摘后再使用加密算法进行报文鉴别。

如果使用密码散列函数产生报文摘要，则攻击者伪造相同报文摘要的原文在计算上是不可行的，因此通过报文摘要能鉴别原文的真实性。而使用普通散列函数产生报文摘要，则攻击者很容易找到与相同报文摘要的其他报文来伪造原文，因此不能通过报文摘要能鉴别原文的真实性。

7-10 计算字符串“SEND1293.BOB”和“SEND9213.BOB”的因特网检验和，看是否完全一样的。

解答：以 16 位（即两个字符）为一组，用反码算术运算求和，任意两组在同一位的数值进行交换都不会改变计算结果，因此“1293”和“9213”的检验和计算结果相同。

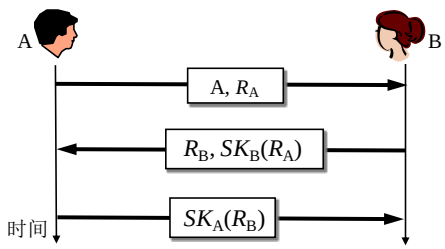
7-11 比较数字签名与报文鉴别码技术的异同。

解答：报文鉴别码和数字签名都能用来保证报文的完整性。

但由于数字签名是产生者用自己的私钥对报文进行加密运算，验证者用产生者的公钥对加密的报文进行验证。报文鉴别码由于双方共享鉴别密钥，因此不能防止鉴别方伪造报文，而数字签名由于使用私钥第报文签名，其他任何人都无法伪造报文。但数字签名计算量比较大。

7-12 请修改图 7-9 中的鉴别协议，使用公钥密码加密算法来实现不重数鉴别协议。

解答：通信双方可以利用自己的私钥对不重数进行签名，并用对方的公钥进行鉴别。SK 表示私钥。




7-13 如果采用信道加密机对网络中所有链路都进行加密，并且所有中间结点（如路由器）也是安全的，是不是就不需在网络其他层次提供安全机制了？

解答：不是。用户的安全性需求是多样的，很难用一种机制满足所有需求。例如，信息

的最终接收者可能需要直接验证信息源的身份，而这种安全需求用逐段的信道加密机很难实现，最好是采用端到端的鉴别机制。

7-14 查看一个无线接入点 AP 的安全配置，看看它都支持几种安全机制。

解答：略

7-15 IPSec 有哪两种运行方式？请简述他们的区别。

解答：IPSec 可以以两种不同的方式运行：传输方式和隧道方式。

在传输方式下，IPSec 保护运输层交给网络层传递的内容，即只保护 IP 数据报的有效载荷，而不保护 IP 数据报的首部。传输方式通常用于主机到主机的数据保护。

在隧道方式下，IPSec 保护包括 IP 首部在内的整个 IP 数据报，为了对整个 IP 数据报进行鉴别或加密，要为该 IP 数据报增加一个新的 IP 首部，而将原 IP 数据报作为有效载荷进行保护。隧道方式通常用于两个路由器之间，或一个主机与一个路由器之间。

7-16 因特网的网络层是无连接的，而 IPSec 是因特网网络层的安全协议，它也是无连接的吗？请说明理由。

解答：IPSec 是有连接的。IPSec 吧因特网传统的无连接网络层转化成了一个具有逻辑连接的层。因为 IPSec 在两个结点之间用 AH 或 ESP 进行通信之前，首先要在这两个结点之间建立一条网络层的逻辑连接，称为安全关联 SA。通过安全关联，双方确定将采用的加密或鉴别算法以及各种安全参数，并在 SA 建立时产生一个 32 位的安全参数索引。目的结点根据 IPSec 报文中携带的 SPI 将其与特定 SA 使用的加密算法和密钥等相关联。

7-17 有了 IPSec 在网络层提供安全服务，为什么还需要运输层和应用层的安全协议？

解答：在 IP 层的安全机制可以为所有主机间提供安全通信服务，但却无法保证用户间电子邮件的安全性。因为利用电子邮件通信的双方并不直接在 IP 层上进行通信，电子邮件需要通过中间的邮件服务器的转发。虽然 IPSec 可以为上层应用提供统一的主机到主机的安全服务，但如果主机上运行多个不同的应用，需要与不同主机进行不同安全需求的通信时，则需要使用运输层的安全协议。

7-18 使用 IPSec 或 SSL 能代替 PGP 为电子邮件提供安全服务吗？

解答：不能，因为利用电子邮件通信的双方并不是直接在 IP 层或运输层上进行通信，电子邮件需要通过中间的邮件服务器的转发。IPSec 或 SSL 都不能为邮件收发双方直接提供安全服务。

7-19 试述防火墙的基本工作原理和所提供的功能。

解答：防火墙是把一个组织的内部网络与其他网络（通常就是因特网）隔离开的软件和硬件的组合。根据访问控制策略，它允许一些分组通过，而禁止另一些分组通过。访问控制策略由使用防火墙的组织根据自己的安全需要自行制订。防火墙作为一种访问控制技术，通过严格控制进出网络边界的分组，禁止任何不必要的通信，从而减少潜在入侵的发生，尽可

能降低内网遭受外网攻击的安全风险。

7-20 是不是在部署了防火墙后，内网的主机就都安全了？

解答：在网络边界位置部署防火墙，对于提高内网安全能够起到积极的作用，但是防火墙技术并不能解决所有的网络安全问题，我们要清楚它在安全防护方面的一些局限性：

防火墙所发挥的安全防护作用在很大程度上取决于防火墙的配置是否正确和完备。

一些利用系统漏洞或网络协议漏洞进行的攻击，防火墙难以防范。

防火墙不能有效防止病毒、木马等通过网络的传播。

分组过滤器不能防止 IP 地址和端口号欺骗，而应用级网关自身也可能有软件漏洞而存在被渗透攻击的风险。

7-21 有了防火墙为什么还需要入侵监测系统？

解答：防火墙试图在入侵行为发生之前阻止所有可疑的通信。但事实是不可能阻止所有的入侵行为，因此需要使用入侵检测系统在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小。IDS 对进入网络的分组执行深度分组检查，当观察到可疑分组时，向网络管理员发出告警或执行阻断操作（由于 IDS 的“误报”率通常较高，多数情况不执行自动阻断）。IDS 能用于检测多种网络攻击，包括网络映射、端口扫描、DoS 攻击、蠕虫和病毒、系统漏洞攻击等。

7-22 入侵检测方法一般可以分为哪两种？它们之间的区别是什么？

解答：入侵检测方法一般可以分为基于特征的入侵检测和基于异常的入侵检测两种。

基于特征的 IDS 维护一个所有已知攻击标志性特征的数据库。每个特征是一个与某种入侵活动相关联的规则集，这些规则可能基于单个分组的首部字段值或数据中特定比特串，或者与一系列分组有关。当发现有与某种攻击特征匹配的分组或分组序列时，则认为可能检测到某种入侵行为。这些特征和规则通常由网络安全专家生成，机构的网络管理员定制并将其加入到数据库中。

基于特征的 IDS 只能检测已知攻击，对于未知攻击则束手无策。基于异常的 IDS 通过观察正常运行的网络流量，学习正常流量的统计特性和规律，当检测到网络中流量某种统计规律不符合正常情况时，则认为可能发生了入侵行为。

7-23 为什么攻击者在进行网络攻击前通常要进行网络扫描？网络扫描有哪几种主要的类型？

解答：在实施网络攻击前，对攻击目标的信息掌握得越全面、具体，越能合理、有效地根据目标的实际情况确定攻击策略和攻击方法，网络攻击的成功率也越高。网络扫描技术是获取攻击目标信息的一种重要技术，能够为攻击者提供大量攻击所需的信息。这些信息包括目标主机的 IP 地址、工作状态、操作系统类型、运行的程序以及存在的漏洞等等。主机发现、端口扫描、操作系统检测和漏洞扫描是网络扫描的四种主要类型。

7-24 在交换式局域网中用嗅探器进行网络监听的困难是什么？交换机毒化攻击的基本原理是什么？如何防范？

解答：由于交换机是根据目的 MAC 地址有目的转发帧，因此分组嗅探器通常仅能接收到发送给自己的帧或广播帧，因此通常无法监听到网络中的其他站点的通信内容。

由于交换机的转发表空间是有限的，并且总是保留最新记录的表项。交换机毒化攻击利用这一特性向交换机发送大量具有不同虚假源 MAC 地址的帧，使这些虚假 MAC 地址表项会填满交换机的转发表，使真正需要被保存的 MAC 地址被更新淘汰。这样该交换机就不得不广播大多数的帧，因为在交换机的转发表中找不到这些帧的目的 MAC 地址。这时，分组嗅探器就能监听到网络中其他主机的通信了。

例如针对交换机毒化攻击，对于具有安全功能的交换机可以在某个端口上设置允许学习的源 MAC 地址的数量，当该端口学习的 MAC 地址数量超过限定数量时，交换机将产生违例动作，从而禁止该端口进行通信。网络管理员还可以禁用交换机的自学习功能，将 IP 地址、MAC 地址与交换机的端口进行静态绑定。

7-25 DDoS 是如何产生巨量攻击流量的？为什么难以防范？

解答：在分布式 DoS 攻击中，攻击者先通过非法入侵手段控制因特网上的许多主机（例如，通过嗅探口令、漏洞渗透、木马等方式），然后控制这些主机同时向攻击目标系统发起 DoS 攻击。很多 DDoS 攻击还结合反射攻击技术进一步将攻击流量进行放大，甚至进行多次反射来产生超巨量的攻击流量。

由于很难区分哪些是恶意分组哪些是正常分组，而且通常参与 DDoS 攻击的分组使用的源 IP 地址都是假冒的，又来找因特网上不同的被控主机，很难追溯到攻击源。因此 DDoS 难以防范。