计算机网络习题与解析(第2版)

鲁文士 著

清华大学出版社

书名：计算机网络习题与解析(第2版)
作者：鲁文士
出版社：清华大学出版社
出版日期：2005年1月
ISBN：7-302-11644-X/TP393-44
定价：32.00元

丛 书 序

劳动就业、岗位技能培训关乎国计民生；全面提高劳动者的就业能力、创业能力和适应职业变化的能力，特别是开展新技术、新岗位的培训，这是时代的大课题。

近年来，各类求职人员特别是各级各类院校毕业生**就业技能匮乏、岗位适应能力欠缺**已是不争的事实。以计算机应用及相关专业为例，大多数毕业生毕业后主要从事面向成熟技术的应用和运作，但一些学校专业教学内容比较陈旧、课程设置不合理的问题日益突出，毕业生**“学校学的用不上，用的大多没学过；说起来似乎什么都懂，做起来什么都不会”**的现象很普遍。同时，社会各类求职人员和在岗人员也有相当部分存在**“实用技能的基本功不扎实，新工作岗位的适应周期长，技术应变能力差，新技术自学能力弱”**等通病。

在这种时代背景下，北京科海培训中心与北京科海电子出版社联手，对用户需求和多媒体视频教学需求进行充分的市场调研，提出“面向岗位，强化技能，盘书互补，学练互动”的全新教学模式，通过整合资源和利用多媒体开发技术优势，精心打造了本套“职场无忧IT技能实训丛书”。

与本丛书配套的多媒体教学光盘由北京科海电子出版社开发，作为2004年“十五”国家规划电子出版物重点选题之一，获相应工程资助。日前，我们的“职场无忧IT技能实训丛书”成功通过专家论证，再次被审定通过为2005年“国家重点音像电子出版工程”项目。

科海将选题重点聚焦在面向应用技能培训的教育市场，“职场无忧IT技能实训丛书”根据广大毕业生就业培训和转岗需要将逐步拓展新技术的各个领域，决心为社会求职者和毕业生求职提供全方位的学习培训。

读者定位

本丛书面向大专院校毕业生求职者和岗位充电者，针对岗位技能进行强化实训指导：

- 针对完成学校教育的人如何获得相关职位提供就业教育
- 为公司在职技术人员掌握新的技能或强化技能提供强化培训

丛书特色

- **模拟实际岗位进行实训：**在书中每一章都精心设计了“岗位技能特训”内容，采用实际岗位项目，模拟岗位真实背景，一切围绕**“全面了解岗位特点、学会做具体工作、快速适应具体工作”**进行。
- 把“应知知识”、“应会技能”、“专家建议”和“岗位能力的强化训练”有机结合，将产品目标定位在“为用而学、学以致用”，以一种**跨媒体**的出版形式（盘书

结合的出版形式）全面指导用户从学校（或其工作岗位）到适应工作岗位到规划自己的职业生涯，并通过网站提供优质服务和交流平台。

本丛书以岗位需求为中心，突出强化实训、实用至上；在编写中严格控制难度、深度，适当拓宽视野；书内书外相结合，应知应会合二为一；职业技能、行业应用并重，基础、方法、技巧并举。

编写内容

本丛书首批推出以下分册：

（1）《3D家装设计岗位技能培训教程》
（2）《电脑平面广告设计岗位技能培训教程》
（3）《网页设计岗位技能培训教程》
（4）《硬件工程师岗位技能培训教程》
（5）《电脑打字员岗位技能培训教程》
（6）《文秘与办公自动化岗位技能培训教程》

我们还将面向以计算机为工具的普及型应用岗位，如机房维护、计算机辅助设计、建筑装潢设计、网络架设与系统管理、电子商务、信息安全、电算化、计算机自动控制、IT设备销售及服务、多媒体制作、计算机信息管理、网络营销、二维三维动画设计等岗位，陆续推出相关教材。

总之，本丛书针对目前最为大众化的IT业应用岗位，通过介绍各岗位的主要应知知识点和应会技能项，将其中各知识点和技能项融入各个章节。与传统培训教程仅介绍知识和技能的情况相比，本丛书更偏重于岗位实用技能的训练，并结合“高手”经验，突出岗位应用特点，不失时机地介绍行业应用中的一些相关背景知识，是求职者和岗位充电者的得力助手。

最后，真诚希望本套丛书能在就业职场助您一臂之力。

技术支持

如果你在学习过程中遇到什么难题，可通过以下方式与我们联系：

信息反馈邮箱：feedback@khp.com.cn
网站支持：http://www.khp.com.cn/zcwy
技术支持电话：010-82896445-8407/06

丛书编委会

2005年2月20日

前　言

“上网”——一个时尚的新概念正悄然融入人们的生活，潜移默化地改变着人们的生活和工作方式。同时，也悄悄地引导着人们进入信息时代。

众所周知，网上的信息都存放在网页上，查看网页信息叫做“浏览”，而设计制作网页的工作人员则称为“网页设计师”。

本书主要围绕网页设计基础、网页设计软件的应用和网页设计制作3个方面来展开岗位技能实训内容。

网页设计基础

网页设计是一个具有挑战性的岗位，需要掌握一些专业化的基础知识。为此，本书安排了一章的内容，重点介绍网页设计的预备知识，包括常用网络术语、网页图像基础、网站分类、网页设计的内容与原则等，还介绍了评价网站的一般方法。

网页设计软件的应用

目前，最简单实用的网页制作方法是使用为设计网页特别定制的可视化网页开发工具来制作网页。本书安排了3章的内容，分别介绍Dreamweaver、Flash、Photoshop这3款软件的基本工具和主要功能，并着重通过实例进行软件操作的强化实训。

网页设计制作

网页设计虽然并非一项高深的技术，但设计的网页应做到简单易读、网站导航功能明确、风格统一、页面容量小等特点。优秀的专业设计师总能设计出不同凡响、富有视觉冲击力的网页，这主要得益于长期的实践训练。为此，本书专门安排了6章，分别对网站规划和布局设计、网页装点设计、网页图片设计、网页按钮设计、动画广告设计和网页综合设计能力等进行了集中强化训练。各章采用了“应知常识点拨-岗位技能指导-设计制作技巧+设计制作特训”的结构，先对设计的基础知识进行点拨，再对实际设计制作技能进行详细指导，然后提供相应的专家经验技巧，最后进行有针对性的设计制作特训。

本书配备一张多媒体光盘，光盘中含有本书所涉及到的全部示例的多媒体演示，以及各个示例所使用的素材，以方便读者在学习过程中查阅和参考。

本书由三创工作室组织编写，陈德荣、刘小伟、周锦智、蒙坪、彭钢、刘飞、王晓霞、李才有参与了资料收集、整理和编写等工作。

由于时间仓促，书中疏漏和不妥之处在所难免，恳请广大读者批评指正。

联系方式：Liuxiao wei@mail.sccvtc.cn

编者

2005年2月

目　录

第 1 章　基本概念和体系结构

本章学习重点

- 典型的网络应用
- 网络服务质量
- 网络成分和性能特征
- 网络协议的分层结构
- 开放系统互连参考模型
- 互连网的TCP/IP协议体系
- 基于OSI的修改模型

1.1　基本知识点

通信网络使得用户能够以话音、视像、电子邮件和计算机文件的形式传递信息。用户使用有线电话或蜂窝电话机、电视机的机顶盒或在计算机上运行的应用程序通过简单的操作规程，就可以请求得到他们所需要的服务。

由通信网络所提供的服务是广泛的：用户通过电话网络可以互相交谈，通过计算机网络可以传送数据，通过电视网络可以看电视节目。因为用户总是通过某种终端设备跟网络交互，所以准确地讲，网络服务是被用户应用（运行在终端设备上的进程）所使用的。

网络设计人员在构建一个网络的时候要互连两种类型的硬件（或称网络元素）：传输链路和路由/交换机。链路从一个地方向另一个地方传输位串。路由/交换机是存储、路由和操作这些位串的计算机。这种硬件支持网络的承载服务，即以某种标准的格式从一个源或用户向一个或多个网络目的地传输位串。承载服务的性能特征跟一些参数有关，它们包括可接受的格式、连接性、从源到目的地路由的选择，以及位串的传输速度、延迟和错误等。

一个网络仅当其承载服务具有必需的特征时才能有效地支持一个特别的用户应用。例如，为了支持话音服务，端到端的延迟应该不大于200毫秒。为了支持数据传输，错误率应该不大于10^{-4}。要求条件很高的应用，比如X射线照影的实时传送（要求具有高的保真度和放射科医师为诊断病案可接受的显示速率）和交互式视频会议，则需要一个高性能的网络。

当用户通过终端设备互相交换信息的时候，所涉及的过程可能是相当复杂的。作为例子，我们考察在两台计算机之间是如何传送一个文件的。首先，在这两台计算机之间必须有一条数据通路，可以是一条直接连接的链路，也可以通过一个通信网络。但是仅此还不够。需要执行的典型任务包括：

（1）源系统必须激活该数据通信通路，或者通知通信网络希望与之通信的目的地系统

的标识。

（2）源系统必须确定，目的地系统已经准备好接收数据。

（3）在源系统上的文件传送程序必须确定，在目的地系统上的文件管理程序已经准备好为这个特别的用户接受并存储文件。

（4）如果在两个系统上的文件格式不兼容，一个或另一个系统必须执行格式翻译功能。

当你浏览WWW时，你启动了一系列的文件传输。

比较复杂的服务可以从具有较少复杂性的服务以层次结构的形式组建。显然，在上述两个计算机系统之间必须有高度的合作。该任务不是实现成单个模块，而是被划分成若干个子任务，每个都单独实现。在协议体系结构中，模块被安排成一个垂直的栈。在协议栈中的每一层都执行为了跟另一通信系统通信所需要的功能的一个相关子集。为了执行比较原始的功能，它需要依赖下一个较低层次，并且遮蔽那些功能的细节。同时，它向上一个较高层次提供服务。在理想的情况下，层次的划分应该使得在一个层次中的修改不需要改变其它的层次。

当然，层次的划分应该让位于不同系统中的两个进程能够通信，因此，这两个系统必须具有同一组层次功能。交流是通过让在两个系统中的对应（或对等）层进行通信而得以实现的。对等层次借助遵从一组规则或约定的格式化数据块进行通信，这组规则或约定就叫做协议。协议主要由语义、语法和定时三部分组成，语义规定通信双方准备“讲什么”，亦即确定协议元素的种类；语法规定通信双方“如何讲”，确定数据的信息格式、信号电平等；定时则包括速度匹配和排序等。

1.1.1 典型的网络应用

WWW是一种分布式的应用，它允许我们浏览一系列通过超链联接的称作Web页面的文档。每个Web页面可以包含正文、图像、音频片段、视频片段以及可能有的链接。一条链接指定在同一文档中的一个位置或者另一个Web页面的位置和名字。位置表示在同一个计算机中或连接到Internet的另一个计算机中的另一个文件。当你点击一条链接（通常表现为突出显示的，例如加亮的或带有下划线的条目）的时候，应用程序会去显示在该文档中的新的位置或传输并显示新的Web页面。

Web页面的大小典型地是从几k字节到几百k字节。如果链接指向一个视频片段或指向一个大的文件，那么就可能要传输几兆个字节。你可能已经经历过，某些Web页面需要等待很长的时间才会显示出来。这种延迟是不难理解的。例如，如果所请求的页面的大小为100k字节，而传送速率只有8kbps，那么传输要化大约两分钟的时间。传输速率不仅受到你的Modem的限制，而且也受到跟你的传输共享某些关键网络链路的其他连接的影响。我们不仅期望Web页面的传送能够快一些，而且要求是无错的。因此可能发生的传输差错应该得以纠正。

在通过网络传输期间，分组可能遭遇可变的延迟，某些分组还可能丢失。作为例子，在开始再现一个声频或视频流之前，目的地需要缓存几个分组。缓存可以吸收掉延迟的波动。就缓冲而言，所有的分组都面临最小等于通过网络延迟的最大值的延迟。确实，为了能够以跟进入网络时同样的恒定间隔输出分组来实现流的再现，所有的分组必须有相同的

总延迟。因此，较快的分组必须被延迟，使得它们有跟最慢的分组相同的延迟。这类应用的传输速率取决于节目的质量。声频传输的速率典型地是从8kbps到30kbps。初级视频则有一个从40kbps到80kbps的速率。对于声频和视频，有一些传输错误是可以接受的，这些差错体现为噪音或图像的失真。好在每秒传送若干帧，只要错误持续的时间不太长，用户的感受就不会很明显。

廉价的视频照相机和音频设备可用来在PC之间建立电话呼叫或视频会议。对于会话，单向延迟如果小于100毫秒，那么就不会被明显地感觉到。该延迟如果达到350毫秒以上，那么就会使会话感到很不舒服。话音的小延迟需求意味着话音采样必须放在小的分组中传输。为了说明这一含义，我们假定话音以64kbps的位流编码。比如说，我们把话音比特放进1 600位长的分组，则收集装满一个分组的比特的时间等于1600/64000 = 25毫秒，分组化引入一个25毫秒的延迟，该延迟加到通过网络的最大延迟。一般说来，允许传输错误所引起的失真要比通过重传错误的分组来纠正错误所需要的过量延迟强。

许多网络应用，从数据库到分布式的日程安排表，到共享的文件服务器，都按照客户/服务器的模型组织。在客户/服务器应用中，服务器被用来回答来自客户的查询。典型地，客户给服务器发送一个查询，等待回答。当回答到达时，客户继续执行自己的程序。对于服务器或网络的故障，客户必须能够检测到，并作出反应。服务器则必须能够处理来自许多个客户的请求。实现这一目标的普遍规程是，让服务器是无状态的，这就意味着服务器不必记住关于先前进行过的查询的任何信息。在实践中，服务器很少是无状态的。然而，应用设计人员总是试图限制服务器必须记住的信息的数量。这类应用的网络需求取决于可以接受的响应时间。

1.1.2　服务质量

用户通过应用程序交换信息。信息传送的特征描述应用产生的交通，也描述在投递这些交通的过程中可以接受的延迟和丢失。

应用产生的信息可以取多种形式：正文，话音，声音，数据，图形，相片，动画和视像。而且，信息传送可以是单工，双工，广播或多投点。

交换的信息可以是模拟的或数字的。例如，有线电视网络投递模拟视频信号给电视机。电话网络在电话机之间传输模拟或数字话音。计算机网络传送比特文件或表示正文、数据、静态图像、声频或视频信号的位流。大多数网络在传送模拟信号时都是先把它们转换成位流。

我们把讨论限于信息的数字传输，因此用户应用最终需要通信网络传输比特文件或位流。我们把这些比特文件或位流称作由用户产生的交通。为了支持用户应用，网络必须能够以满意的方式传输由应用产生的交通。

需要注意的是，由视频信号产生的位流依赖于所采用的压缩方案可能变化很大。把一页正文编码成ASCII字符串仅产生一个2k字节的串；当该页被数字化成像素，并且以传真的方式压缩时，它将产生一个50k字节的串。一幅彩色相片的高质量数字化（类似于好的彩色激光打印机的质量）产生33.5M字节串；一幅黑白相片的低质量数字化产生0.5M字节串。

我们可以把所有的交通划分成3种类型。用户应用可能产生一个恒定位速率（CBR流），

一个可变位速率（VBR）流，或一个具有不同时序特征的报文序列。

为了发送话音信号，电话网络设备先把它转换成一个恒定的64kbps速率的位流。一些视频压缩标准也把视频信号转换成具有恒定位速率（CBR）的位流。例如，MPEG1就是一个把视频压缩成一个恒定位速率流的一个标准。压缩位流的速率取决于为压缩算法所选择的参数，例如，视频窗口的大小，每秒帧数以及量化级的数目。MPEG1使用1.5Mbps产生较差质量的视频图像，使用3Mbps产生好的图像质量。

话音信号的速率范围是从大约4kbps（重型压缩和低质量）到64kbps。声音信号的速率范围是从8kbps到大约1.3Mbps（CD质量）。对于具有可接受的质量的音频或视频应用，网络必须以短的延迟和少遭破坏的条件（至多有一小部分的位被破坏）传输位流（被破坏的部分称作位错率即BER）。

对于实时视频和语音会话，端到端的延迟应该小于200毫秒，因为大的延迟会使人感到不舒服。对于交互式视频和点播信息这类非实时的交互应用，延迟可以是几秒。对于诸如视频或声频节目分发这样的非交互应用，延迟不是关键的因素。

对于声频和视频传输，在不压缩的情况下的最大的可接受的位错率是10^{-4}。然而，当压缩声频和视频信号时，在被压缩的信号中的差错会引起解压缩信号的一系列差错。因此，传输压缩信号能够容忍的差错要比10^{-4}小得多。

一些信号压缩技术把信号转换成具有可变位速率（VBR）的位流。例如，MPEG2就是针对视频信号可变位速率压缩的一个系列标准。当压缩电影的场景快速移动时，其位速率就要比慢速移动时大。直接广播卫星（DBS）使用MPEG2，其平均位速率等于4Mbps。

为了描述VBR流的特征，网络工程师需要指定平均位速率，并说明该位速率的波动情况。相关应用可以接受的延迟和位错率类似于CBR应用。

在网络上的许多应用都通过交换报文的进程来实现。我们可以把报文看成是一个可变长度的位串。例如，当浏览Web时，用户向服务器发送一个Web、声频/视频片段或文档请求。服务器通过给用户发送所请求的记录进行应答。作为另一个例子，分布式计算应用产生远地过程调用，然后远地机器返回该过程执行的结果。

由各种用户应用产生的报文交通可以具有一个广大范围的特征。一些应用，例如电子邮件，产生分离的报文。另一些应用，例如分布式计算，产生长的报文流。不同应用和设备所产生的报文速率可能差别很大。

为了刻画由一个产生报文流的应用所形成的交通的数量，网络工程师可以像在VBR规范中所做的那样，指定平均交通速率和该速率的波动值。

网络必须以可接受的延迟传送报文，并且只可以破坏报文的一小部分。典型的可接受的延迟值，对于实时应用是200毫秒，对于交互式服务是几秒，对于像是电子邮件这样的非交互式服务则是许多秒。可接受的部分报文被破坏的比例，对于数据传输可以是1:10~1:8，而对于诸如邮件分发这样的非关键应用可以是大得多的值。

在交换报文序列的应用中，我们还可以区分两种应用。一种是希望报文按照正确的顺序到达目的地，另一种则不在乎报文到达的顺序。

应用对网络的其他需求主要有可靠性和安全性。当一条或多条链路或交换机失效时，网络将不能够在源和目的地之间提供连接，直到这些故障被修复为止。可靠性是指这类故障发生的频率和持续时间。某些应用，例如发电厂的控制、医院生命支持系统和关键的银

行操作，需要非常可靠的网络操作。典型地，我们希望在几个指定的源和目的地之间提供比较高的可靠性。较高的可靠性可以通过在指定的节点对之间提供互不重叠的路由取得。

像在以太网这样的多路访问的网络中，每个计算机都“听到”在网络上传输的每个分组。无线电话传输的情况也类似。在这些网络中，为保证传输的保密要求，需要对传输加密。一般说来，安全性关心为防止对数据或信息传送的非授权访问所采取的步骤。随着钱币和其他财富采取在网络上传送的电子单据的形式，安全性的问题变得越来越紧迫。

1.1.3　网络成分和性能特征

一个通信网络是互相连接在一起并被管理的网络成分的集合，它能够把信息从在一个节点上的一个用户传送到在另一个节点上的另一个用户。下面我们讨论主要的网络成分，考察这些成分是如何影响它们所实现的服务的特征的。

主要的网络成分是传输链路和路由/交换机。链路把位流以某种速率、给定的位错率和固定的传播时间从一端传送到另一端。最重要的链路是光纤、铜线、同轴电缆和微波（或无线）链路。光纤和铜线链路通常是点到点的链路，而无线链路通常是广播链路。多条输入和输出链路都端接到路由/交换机。路由/交换机是把位从其输入链路传送到输出链路的设备。每当输入位速率超过输出位速率时，过量的位就被缓冲在路由/交换机中。

对于网络成分互连的另一个非常重要的视野由队列网络模型提供。考虑一个具有n条输入链路和m条输出链路的路由/交换机，如图1-1所示，其右边的图是队列模型。每条输入链路的接收方都往其输入缓冲区写数据，每条输出链路的发送方都从其输出缓冲区读数据。路由/交换机把位或分组从输入缓冲区传送到适当的输出缓冲区。这种关于路由/交换机和链路的队列网络模型被用来描述和评价网络性能。例如，一个分组在一个输出缓冲区中遭遇的队列延迟跟在该缓冲区中排在该分组前面的分组的个数成正比。计算队列延迟和分组丢失是一件困难的事情。

由源产生的一个分组在一条链路上传输，在一个路由/交换机处被缓冲，然后选择路由前往另一条链路，如此继续下去，直到它抵达目的地为止。分组通过网络经历的延迟取决于组成网络的成分、通过这些元素的交通以及网络运行的方式。

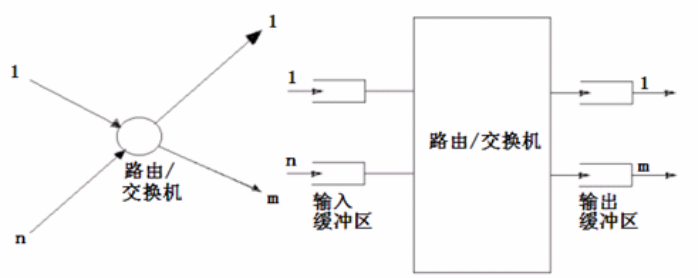


图 1-1　路由/交换机和队列网络模型

对通过网络的延迟的具体分析可能是相当复杂的。现在，我们可以把总延迟分解成4个部分：

总延迟 = 发送延迟+传播延迟+队列延迟+处理延迟 （1-1）

其中，发送延迟是发送一个分组所需要的时间，因此

发送延迟 = 分组大小/发送速度 （1-2）

例如，对于一个10 000位的分组和1Mbps的发送速度，发送延迟等于10毫秒。

传播延迟是信号传播的时间，因此

传播延迟 = 从源到目的地的距离/电或光信号的速率 （1-3）

每公里电或光信号的传播时间是在3.3微秒到5微秒之间。队列延迟是在路由/交换机中的排队延迟。每当进入路由/交换机的交通的位速率超过输出链路的容量时，就会发生队列延迟。过量的位在路由/交换机的缓冲区中排队。跟前面的两个延迟因素相比，队列延迟显著地受网络控制策略的影响。最后，处理延迟是网络路由/交换机所需要的处理时间。通常，这种处理时间相对较小，我们将假定该处理延迟可以忽略。

假定作为一个粗略的常规，网络控制的结果是每个进入交换机的分组都要等待平均4个分组的发送时间。那么，平均队列延迟是4倍的发送延迟，即

总延迟 = 5*发送延迟+传播延迟 （1-4）

结合式（1-2）和（1-4），我们可以看出，总延迟依赖于发送速率和链路的长度，也依赖于分组的大小。

1.1.4 协议的分层结构

两个系统中实体间的通信是一个十分复杂的过程，为了减少协议设计和调试过程的复杂性，大多数网络的实现都按层次的方式来组织，每一层完成一定的功能，每一层又都建立在它的下层之上。不同的网络，其层的数量、各层的名字、内容和功能不尽相同，然而在所有的网络中，每一层都是通过层间接口向上一层提供一定的服务，而把这种服务是如何实现的细节对上层加以屏蔽。

更具体地讲，层次结构包括以下几个含义：

- 第n层的实体在实现自身定义的功能时，只使用（n-1）层提供的服务。
- n层向（n+1）层提供服务，此服务不仅包括n层本身所执行的功能，还包括由下层服务提供的功能总和。
- 最低层只提供服务，是提供服务的基础；最高层只是用户，是使用服务的最高层；中间各层既是下一层的用户，又是上一层服务的提供者。
- 仅在相邻层间有接口，且下层所提供服务的具体实现细节对上层完全屏蔽。

N层中的活动元素通常称为n层实体。不同机器上同一层的实体叫做对等实体。N层实体实现的服务为n+1层所利用。在这种情况下，n层被称为服务提供者，n+1层是服务用户。服务是在服务访问点（SAP）提供给上层使用的。N层SAP就是N+1层可以访问N层服务的地方。每个SAP都有一个能够唯一地标识它的地址。在同样的意义上，我们可以把电话系统中的电话插孔看成是一种SAP，而SAP地址就是这些插孔的电话号码。要想和他人通话，

就必须知道他的SAP地址（电话号码）。类似地，在邮政系统中，SAP地址是街名和信箱。发一封信，必须知道收信人的SAP地址。

相邻层之间要交换信息，在接口处也必须遵循一定的规则。在典型的接口上，n+1层实体通过SAP把一个接口数据单元（IDU）传递给n层实体。IDU由服务数据单元（SDU）和一些控制信息组成。SDU是将要跨越网络传递给远方对等实体，然后上交给远方n+1层的信息。控制信息被下层实体用来指导其功能任务的执行，但不是发送给远方对等实体的内容。

为了传送SDU，n层实体可能把SDU分成几段，每一段加上一个头之后作为一个独立的协议数据单元（PDU）送出。PDU被对等实体用于执行对等协议。对等实体根据PDU头部的信息分辨哪些PDU包含数据，哪些PDU包含控制信息，以及哪些PDU提供顺序号和计数等。

下层向上层提供的服务可以划分为面向连接的和无连接的两大类别。面向连接的服务类似于打电话。要和某个人通话，我们先拿起电话，拨号码，谈话，然后挂断。同样，在使用面向连接的服务时，用户首先要建立连接，传送数据，然后释放连接。连接本质上象个管道，发送者在管道的一端放入物体，接收者在另一端以同样的次序取出物体。

相反，无连接服务类似于邮政系统中普通信件的投递。每个报文（信件）带有完整的目标地址，并且每一个报文都独立于其它报文，经由系统选定的路线传递。在正常情况下，当两个报文发往同一目的地时，先发的先收到。但是，也有可能先发的报文在途中延误了，后发的报文反而先收到。而这种情况在面向连接的服务中是绝不可能发生的。

无确认无连接的服务称作数据报服务。电报服务与此类似，它不向发送者发回确认消息。在某些情况下，可能既希望免除建立连接的麻烦，又要求确保信息传送的可靠。此时，可以选用有确认的数据报服务。这很象寄出的一封挂号信又要求回执一样。当收到回执时，寄信人有绝对的把握相信信件已到达目的地而没有在途中丢失。

还有一种服务叫做“请求—应答”服务。使用这种服务时，发送者传送一个查询数据报，应答数据报则包含回答信息。例如，我们向图书馆询问某本书是否已经借出就属于这类情况。“请求—应答”服务通常被用于客户—服务器模式下的通信：客户发出一个请求，服务器作出响应。

服务在形式上是由一组原语（Primitive）来描述的。这些原语供用户和其它实体访问该服务时调用。它们通知服务提供者采取某些行动或报告某个对等实体的活动。

应该指出，服务和协议是完全不同的概念，但二者又常常被混淆在一起。它们之间的区别是如此重要，以致于我们在此必须再强调一次。服务是各层向它的上层提供的一组原语。尽管服务定义了该层能够为它的上层完成的操作，但丝毫也未涉及这些操作是如何完成的。服务定义了两层之间的接口，上层是服务用户，下层是服务提供者

与之相对比，协议是定义在相同层次的对等实体之间交换的帧、分组和报文的格式及含义的一组规则。实体利用协议来实现它们的服务定义。只要不改变提供给用户的服务，实体可以任意地改变它们的协议。这样，服务和协议就被完全地分离开来。

1.1.5　OSI参考模型

OSI参考模型如图1-2所示。该模型基于国际标准化组织（ISO）的建议，是作为要对各

种层次上使用的网络协议实现国际标准化的工作的第一步而提出来的。它的提出是要为协调标准的研制提供一个共同的基础，允许现存的和正在演变的标准化活动有一致的框架和前景。其最终目的是，允许任一支持某种可用标准的计算机的应用进程自由地与任何支持同一标准的计算机的应用进程进行通信，而不管计算机是由哪个厂商制造的。正因为如此，该模型被称为开放系统互连（OSI）参考模型。

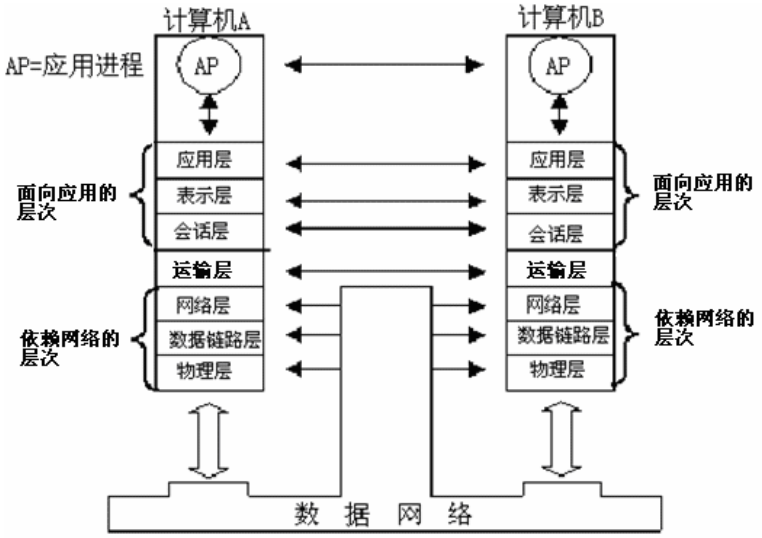


图 1-2　OSI 参考模型总体结构

OSI参考模型把整个通信子系统被划分为七个层次，每层执行一种明确定义的功能。从概念上讲，这些层可以被看成执行两类功能，即依赖于网络的功能和面向应用的功能。最低3层（1-3）是依赖网络的，牵涉到将两台通信计算机链接在一起所使用的数据通信网的相关协议。高三层（5-7）是面向应用的，牵涉到允许两个末端用户应用进程交互作用的协议，通常是由本地操作系统提供的一套服务。中间的运输层为面向应用的上3层遮蔽了跟网络有关的下3层的详细操作。本质上讲，它建立在由下3层提供的服务上，为面向应用的高层提供网络无关的信息交换服务。

每一层的功能以协议形式正规描述，协议定义了某层跟另一（远方）系统中的一个类似层（对等层）通信所使用的一套规则和约定。每一层向相邻上层提供一套确定的服务，并且使用由相邻下层提供的服务向远方对等层传输跟该层协议相关的信息单元。例如，运输层为它上面的会话层提供可靠的网络无关的信息传输服务，并且使用其下面网络层所提供的服务将与运输层协议有关的一组信息单元传送给另一系统中的一对等运输层。在概念上，每一层都根据一个明确定义的协议跟一个远方系统中的一个类似对等层通信，但在实际上该层所产生的协议信息单元是借助于相邻下层所提供的服务传送的。

下面我们就从最下层开始，逐次介绍OSI参考模型的各层。请注意，OSI模型本身并未确切地描述用于各层的具体服务和协议，它仅仅告诉我们每一层应该做什么。

物理层（physical layer）涉及到通信在信道上传输的原始比特流。设计上必须保证一方发出二进制“1”时，另一方收到的也是“1”而不是“0”。这里的典型问题是用多少伏特电压表示“1”，多少伏特电压表示“0”；一个比特持续多少微秒；传输是否在两个方向上

同时进行；最初的物理连接如何建立和完成通信后连接如何终止；网络接插件有多少针以及各针的用途。这里的设计主要是处理机械的、电气的和过程的接口，以及物理层下面的物理传输介质问题。

数据链路层（data link layer）指定在网络上沿着网络链路在相邻节点之间移动数据的技术规范。它的主要任务是加强物理层传输原始比特的功能，使之对网络层显现为一条无错线路。发送方把输入数据分装在数据帧（data frame）里（典型的帧为几百字节或几千字节），按顺序传送各帧，并且有可能要处理接收方回送的确认帧（acknowledgement frame）。因为物理层仅仅接收和传送比特流，并不关心它的意义和结构，所以只能依赖各链路层来产生和识别帧边界。可以通过在帧的前面和后面附加上特殊的二进制编码模式来达到这一目的。如果这些二进制编码偶然在数据中出现，则必须采取特殊措施以避免混淆。

网络层（network layer）关系到子网的运行控制，其中一个关键问题是确定分组从源端到达目的端的路由。路由选择可以使用网络中固定的静态路由表，路由几乎保持不变；也可以在每一次会话开始时决定（例如通过终端对话决定）；还可以根据当前网络的负载状况，高度灵活地为每一个分组决定路由。如果在子网中同时出现过多的分组，它们将相互阻塞通路，形成瓶颈。此类拥塞控制也属于网络层的功能范围。

运输层（transport layer）的基本功能是从会话层接收数据，并且在必要时把它分成较小的单位，传递给网络层，并确保到达对方的各段信息正确无误，而且，这些任务都必须高效率地完成。从某种意义上讲，运输层使会话层不受硬件技术变化的影响。运输层是真正的从源到目标的“端到端”的层。源端机上的某程序，利用报文头和控制报文与目标机上的类似程序进行对话。而在运输层以下的各层中，协议是每台机器包括中间节点都要参照执行的协议，而不是最终的源端机与目标机之间的协议。通常在它们中间可能还有多个路由器，这些路由器都要对路过的信息块进行1~3层的处理。也就是说，1层~3层是链接起来的，4层~7层是端到端的。

会话层（session layer）允许不同机器上的用户建立会话（session）关系。会话层允许进行类似运输层的普通数据传输，并提供了对某些应用有用的增强服务会话，也可被用于远程登录到分时系统或在两台机器间传递文件。会话层服务之一是管理对话。会话层允许信息同时双向传输，或任一时刻只能单向传输。若属于后者，则类似于单线铁路，会话层将记录此时该轮到哪一方了。一种与会话有关的服务是令牌管理（token management）。有些协议保证双方不能同时进行同样的操作，这一点很重要。为了管理这些活动。会话层提供了令牌。令牌可以在会话双方之间交换，只有持有令牌的一方可以执行某种关键操作。另一种会话服务是同步（synchronization）。如果网络平均每小时出现一次大故障，而两台计算机之间要进行长达两小时的文件传输时该怎么办？每一次传输中途失败后，都不得不重新传输这个文件。而当网络再次出现故障时，又可能半途而废了。为了解决这个问题，会话层提供了一种方法，即在数据流中插入检查点。每次网络崩溃后，仅需要重传最后一个检查点以后的数据。

表示层（presentation layer）完成某些特定的功能，由于这些功能常被请求，因此人们希望找到通用的解决办法，而不是让每个用户来实现。值得一提的是，表示层以下的各层只关心可靠地传输比特流，而表示层关心的是所传输的信息的语法和语义。表示层服务的一个典型的例子是用一种大家一致同意的标准方法对数据编码。大多数用户程序之间并不

是交换随机的比特流，而是诸如人名、日期、货币数量和发票之类的信息。这些对象是用字符串、整型、浮点数的形式，以及由几种简单类型组成的数据结构来表示的。不同的机器用不同的代码来表示字符串（如ASCII和Unicode）和整型（如二进制反码和二进制补码）等。 为了让采用不同表示法的计算机之间能进行通信，交换中使用的数据结构可以用抽象的方式来定义，并且使用标准的编码方式。表示层管理这些抽象数据结构，并且在计算机内部表示法和网络的标准表示法之间进行转换。

应用层（application layer）包含大量人们普遍需要的协议。所有虚拟终端软件都位于应用层。另一个应用层功能是文件传输。此外还有电子邮件、远程作业录入、名录查询和其它各种通用和专用的功能。

1.1.6 TCP/IP协议体系

TCP/IP（Transmission Contol Protocol / Internet Protocol）是传输控制协议/互连网络协议的缩写，当初是为美国国防部高级研究计划局（DARPA）设计的，一般称为ARPAnet，其目的在于能够让各种各样的计算机都可以在一个共同的网络环境中运行。

图1-3示出了TCP/IP的分层结构及其与OSI七层协议模型的对应关系。网络接口层似乎与OSI的数据链路层和物理层相对应，但实际上TCP/IP本身并没有真正描述这一部分，只是指出主机必须使用某种协议与网络连接，以便能在其上传递IP（互连网络协议）分组。具体的物理网络可以是各种类型的局域网，如以太网、令牌环网、令牌总线网等，也可以是诸如X.25、帧中继、电话网、DDN等公共数据网络。网络接口层负责从主机或节点接收IP分组，并把它们发送到指定的物理网络上。

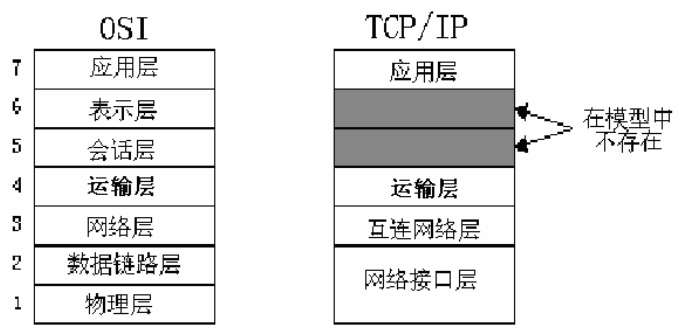


图 1-3　TCP/IP 体系结构

互连网络层是整个体系结构的关键部分，它的功能是使主机可以把分组发往任何网络，并使分组独立地传向目的地（可能经由不同的物理网络）。这些分组到达的顺序和发送的顺序可能不同，因此如需要按顺序发送及接收时，高层必须对分组排序。必须注意到，我们所说的“internet”是基于一般意义的，虽然Internet（因特网）中确实存在互联网络层。

互连网络层定义了标准的分组格式和协议，即IP协议（internet protocol）。互连网络层的功能就是把IP分组发送到应该去的地方。选择分组路由和避免阻塞是这里主要的设计问题。由于这些原因，我们有理由说TCP/IP互连网络层和OSI网络层在功能上非常相似。

运输层在TCP/IP模型中位于互连网络层之上，它的功能是使源端和目的端主机上的对

等实体可以进行会话（和OSI的运输层一样）。这里定义了两个端到端的协议。第一个是传输控制协议TCP（Transmission Control Protocol）。它是一个面向连接的协议，允许从一台机器发出的字节流无差错地发往互联网上的其它机器。它把输入的字节流分成报文段，并传给互连网络层。在接收端，TCP接收进程把收到的报文再组装成输出流。TCP还要处理流量控制，以避免快速发送方向低速接收方发送过多报文而使接收方无法处理。

第二个协议是用户数据报协议UDP（User Datagram Protocol）。它是一个不可靠的、无连接协议，用于不需要TCP的排序和流量控制能力而是自己完成这些功能的应用程序。它也被广泛地应用于只有一次的客户—服务器模式的请求—应答查询，以及快速递交比准确递交更重要的应用程序，如传输语音或影像。IP、TCP和UDP之间的关系如图1-3所示。自从这个协议体系出现以来，IP已经在很多其它网络上实现了。

运输层的上面是应用层。它包含所有的高层协议。最早引入的是虚拟终端协议（TELNET）、文件传输协议（FTP）和电子邮件协议（SMTP），如图1-13所示。虚拟终端协议允许一台机器上的用户登录到远程机器上进行工作，文件传输协议提供了有效地把数据从一台机器移动到另一台机器的方法。电子邮件最初仅是一种文件传输，但是后来为它提出了专门的协议。这些年来又增加了不少协议，例如域名系统服务DNS（domain name service）用于把主机名映射到网络地址；还有HTTP协议，用于在环球网（WWW）上获取主页等。

1.1.7　一个基于OSI的修改模型

不管OSI模型和协议，还是TCP/IP模型和协议，都不是十全十美的，对它们都有不少的批评意见。OSI的会话层对许多应用都没有用，表示层内容又很少。实际上，当初英国的ISO提案仅有5层，而不是7层。与会话层和表示层相比，数据链路层和网络层功能是太多了，后来又不得不把它们分成几个子层，每个子层都有不同的功能。

TCP/IP模型和协议也有自己的问题。首先，该模型没有明显地区分服务、接口和协议的概念。良好的软件工程实践要求区分规范和实现。因此，在使用新技术来设计新网络问题上，TCP/IP模型不是一个很好的模板。第二，TCP/IP模型完全不是通用的，并不适合描述除TCP/IP体系之外的任何协议栈。例如，试图用TCP/IP模型描述SNA几乎是不可能的。第三，网络接口层在分层协议中根本不是通常意义下的层。它只是一个接口，处于网络层和链路层之间。接口和层之间的区别是很大的，不能混淆起来。第四，TCP/IP模型不区分（甚至不提及）物理层和数据链路层。这两层完全不同。好的模型应把它们作为分离的层，而TCP/IP模型并没有这样做。

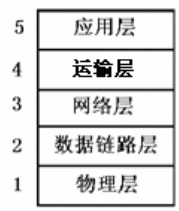


图 1-4　一个使用的网络参考模型

尽管存在着这样那样的缺点，OSI模型（去掉会话层和表示层）对于讨论计算机网络还是特别有用的。但是OSI协议并未流行。TCP/IP协议体系正好相反，模型实际上不存在，但协议被广泛使用。从应用的方面考虑，在当前实际的工作中人们经常使用修改的OSI模型，但主要讨论TCP/IP网络和相关的协议，以及诸如帧中继、SONET和ATM等新的协议。事实上，现在人们普遍使用图1-4所示的五层模型作为本课程的框架。

1.2 基本练习题

1．一个“客户-服务器”系统的性能受到两个网络因素的影响：网络带宽（每秒传输多少位）和延迟（第1位从客户传播到服务器花多少秒的时间）。试给出一个具有高带宽高延迟的网络的例子，再给出一个具有低带宽低延迟的网络的例子。

解答：跨洲的光纤链路可能具有每秒若干个千兆位的带宽，但由于光在数千公里的距离上传播，延迟值也会很高。相反呼叫在同一建筑物内的一台计算机的一条56kbps的modem链路具有低的带宽和低的延迟。

2. 一个“客户-服务器”系统使用卫星网络，卫星的高度是40，000公里，试问就对请求的响应而言，最好情况的延迟是多少？

解答：请求必须上行和下行，响应也必须上行和下行，因此经过的总的通路长度是40，000×4 = 160，000公里。光在空气和真空中的速度是300，000公里/秒，仅传播延迟就等于160，000÷300，000≈0.533秒，即533毫秒。

3. 除了带宽和延迟，还需要什么其它的参数，才能很好地特征化一个用于数字化话音交通的网络所提供的服务质量？

解答：话音需要均匀的投递时间，因此在网络中抖动的时间量是重要的。这可能被表示成标准的投递时间偏移。延迟短但变化大的条件实际上要比延迟长一些但变化小的条件更坏。

4. 试说明队列头阻塞的含义。

解答：队列头阻塞的发生意味着在缓冲区中积累起来的等待到同一输出的分组阻止排其后的其它分组得到前往它们的输出端的机会。

5. 什么是输出阻塞？

解答：在输出阻塞的情况下，两个输入竞争同一输出端口，其中有一个将得不到对输出的访问。

6．局域网的一个替代方案是大型的分时系统，该分时系统带有许多个终端，连接所有的用户。请给出使用局域网的客户-服务器系统的两个优点。

解答：局域网模型可以递增扩展，且整个系统不会因单点故障而崩溃（如果有备份服

务器的话）。它可能会廉价一些（低成本），并提供更多的计算能力和更好的交互式接口。

7. 举出使用分层协议的两条理由。

解答：通过协议分层可以把设计问题划分成较小的易于处理的片段。分层意味着某一层的协议的改变不会影响较高层或较低层的协议。

8．一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字节长的协议头。那么，网络带宽中有多大比率用于协议头信息的传输？

解答：总共有n层，每层加h字节，在每个报文上附加的头字节的总数等于hn，因此头消耗的有关空间所占的网络带宽的比率为hn / (M+hn)

9. 给出分组元数据的例子。

解答：作为元数据信息的一个例子是包含在一个分组的头段中的目标和源地址。对于桥接器和交换机而言，这些地址是MAC地址。

10. 在计算机网络中术语编址的含义是什么？

解答：在计算机网络中把具有唯一性的地址分配给不同的网络设备的过程叫做编址（addressing）。

11. 在计算机网络中术语命名的含义是什么？

答：命名是为设备分配一个具唯一性的网络名字的过程。

12. 选择题

网络体系结构可以定义成：

a. 一种计算机网络的实现
b. 执行计算机数据处理的软件模块
c. 建立和使用通信硬件和软件的一套规则和规范
d. 由ISO（国际标准化组织）制定的一个标准

解答：c

13. 选择题

下列那一项描述了网络体系结构中的分层概念？

a. 保持网络灵活且易于修改
b. 所有的网络体系结构都使用相同的层次名称和功能
c. 把相关的网络功能组合在一层中
d. a 和 c

解答：d

14. 在OSI的第几层分别处理下面的问题？

（a）将待传输的比特流划分成帧
（b）决定使用哪条路径通过子网
（c）传输线上的位流信号同步
（d）两端用户间传输文件

解答：（a）第二层（数据链路层）将待传输的比特流划分成帧
（b）第三层（网络层）决定使用哪条路径通过子网
（c）第一层（物理层）处理传输线上的位流信号同步
（d）第七层（应用层）处理两端用户间的文件传输

15. 选择题

在下列功能中，那一个最好地描述了OSI（开放系统互连）模型的数据链路层？

a. 保证数据正确的顺序、无错和完整
b. 处理信号通过媒体的传输
c. 提供用户跟网络的接口
d. 控制报文通过网络的路由选择

解答：a

16. 选择题

OSI模型的物理层负责下列哪一种功能？

a. 格式化报文
b. 为数据选择通过网络的路由
c. 定义连接到媒体的特征
d. 提供远程文件访问能力

解答：c

17. 选择题

ISO提出OSI模型是为了：

a. 建立一个设计任何网络结构都必须遵从的绝对标准
b. 克服多厂商网络固有的通信问题
c. 证明没有分层的网络结构是不可行的
d. a 和 b
e. 上列陈述都不是

解答：b

18. 选择题

在不同网络节点的对等层之间的通信需要下列哪一项？

a. 模块接口
b. 对等层协议
c. 电信号
d. 传输媒体

解答：b

19. 试描述OSI模型中的信息流动的过程。

解答：发送进程有些数据要传给接收进程，它把数据交给了应用层，应用程序在数据前面加上应用层报头，即应用层的协议控制信息，再把结果交给表示层。表示层可能以各种方式对应用层的报文进行格式转换，并且可能也要在报文前面加上一个协议控制信息（报文头），并把所得的结果交给会话层。有一点在这里是很重要的，即表示层并不知道而且也不应该知道应用层交给它的数据中哪一个部分是应用层的头，哪一个部分是真正的用户数据。

这一过程重复进行下去，亦即当报文通过源节点的各个网络层次时，每层的协议实体都给它加上控制信息。报文抵达源节点的物理层之后，信息以物理信号的形式通过物理链路发射。报文通过物理线路到达网络中的第一个中转节点，在那里向上通过三个层次到了网络层后返回，接着又在第二条物理链路上被送往下一个中转节点。这个过程在网络中沿信息传送路经反复进行直到报文抵达目标节点。在接收机里，当信息向上传递时，各种协议控制信息被一层一层地剥去。最后数据到达接收进程。

整个过程中最关键的概念是，虽然数据的实际传输方向是垂直的，但每一层在进行程序设计时都好象数据一直是水平传输的。例如，当发送方的运输层从会话层得到报文时，它加上一个运输层报头，并把报文发送给接收方的运输层。从发送方运输层的观点来看，实际上它必须把报文传给本机内的网络层，但这一事实只是不重要的技术细节。如同一位说非通用语的外交官在联合国发言时，他认为自己是在向在座的其他外交官致词。事实上，他仅是在向自己的翻译讲话，也许只有翻译能够明白他在讲什么内容；然而这并不妨碍他和别的外交官交流，因为这仅仅是一个技术细节。

20. 在下列每一个OSI层的名称前面标上一个正确的字母序号，使得每一个名称跟你认为最恰当的描述相匹配。

_____应用层_____表示层_____会话层_____运输层_____网络层
_____数据链路层_____物理层

a. 指定在网络上沿着网络链路在相邻节点之间移动数据的技术
b. 在通信应用进程之间组织和构造交互作用
c .提供分布式处理和访问
d. 在由许多开放系统构成的环境中允许在网络实体之间进行通信
e. 将系统连接到物理通信媒体
f. 协调数据和数据格式的转换，以满足应用进程的需要
g. 在端点系统之间传送数据，并且有错误恢复和流控功能

解答：

c 应用层 f 表示层 b 会话层 g 传输层 d 网络层
a 数据链路层 e 物理层

21．在下列每个空白处填上一个阿拉伯数字（1-6），表示在源节点的一个用户发送一个信息给在目标节点的一个用户所发生的事件的顺序。

____当信息通过源节点时，每一层都给它加上控制信息
____在源节点的网络用户产生信息
____在目标节点的网络用户接收信息
____信息向上通过目标节点的各个网络层次，每一层都除去它的控制信息
____信息以电信号的形式通过物理链路发射
____信息传给源节点的最高层（OSI 模型的应用层）

解答： 3 当信息通过源节点时，每一层都给它加上控制信息
1 在源节点的网络用户产生信息
6 在目标节点的网络用户接收信息
5 信息向上通过目标节点的各个网络层次，每一层都除去它的控制信息
4 信息以电信号的形式通过物理链路发射
2 信息传给源节点的最高层（OSI 模型的应用层）

22. 有确认服务和无确认服务之间的差别是什么？在下列情况下，请说出哪些可能是有确认服务或无确认服务？哪些两者皆可？哪些两者皆不可？

a）连接建立
b）数据传输
c）连接释放

解答：在有确认服务中，作为对请求原语的反应，接收方要发出一个明确的响应原语。具体地讲，有确认服务包括请求、指示、响应和证实4个原语，而无确认服务则只有请求和指示2个原语。连接服务总是有确认服务，因为远程对等实体必须同意才能建立连接。在所给出的3个例子中，（a）必须是有确认服务；取决于网络设计者的选择，（b）和（c）可以是有确认服务，也可以是无确认服务。

23. TCP/IP位于OSI模型的什么层次？

答：TCP/IP中最主要的协议IP位于OSI模型的第3层，即网络层。然而实际上，TCP/IP是由许多独立的协议组成的一个协议族。它包括运行在相当于OSI第4层（运输层，也称传输层）的TCP和UDP。运输层的上面是应用层。它包含所有的高层协议。最早引入的是虚拟终端协议（TELNET）、文件传输协议（FTP）和电子邮件协议（SMTP）。后来又增加了不少协议，例如域名系统服务DNS（domain name service）用于把主机名映射到网络地址；NNTP协议，用于传递新闻文章；还有HTTP协议，用于在环球网（WWW）上获取主页等。

总起来讲，TCP/IP的应用层相当于OSI的最高3层，即会话层、表示层和应用层的结合。在TCP/IP协议族中还有许多协议是专门设计用来执行管理功能的，例如ICMP就是这样的一个协议；也有的协议是用来方便层间通信的，例如ARP和DNS就属于这类协议。

24. 什么是服务原语？服务原语的三要素是什么？服务原语的类型有哪几种？

解答：服务原语是一层对它向其相邻上层所提供的服务的描述的形式，每个原语都带有一套相关的服务参数。服务是通过一组服务原语来执行的，原语供用户和其它实体访问该服务时调用。它们被用来通知服务提供者采取某些行动或向其相邻上层报告某个对等实体的活动。原语包括原语类型、被呼和主呼地址、以及用户数据三个主要元素，原语名字则包含原语类型和提供服务的层的标识，如T_CONNECT.request是由传输服务用户——即会话层——发出的一个请求原语，其目的是要跟远方用户（会话层）建立一种（逻辑的）传输连接。S_DATA. indication是由对等（通信）会话层发给它上面的表示层的一个指示原语，并且涉及从远方表示层收到的数据。

服务原语的类型有请求原语、指示原语、响应原语和证实原语。

1.3　综合应用练习题

1. 在下列情况下，计算传送1000KB文件所需要的总时间，即从开始传送时起直到文件的最后一位到达目的地为止的时间。假定往返时间RTT是100毫秒，一个分组是1KB（即1024字节）的数据，在开始传送整个的文件数据之前进行的起始握手过程需要2×RTT的时间。

（a）带宽是1.5Mbps，数据分组可连续发送。

解答：2个起始的RTT：100×2=200毫秒

传输时间：RTT÷2=100÷2=50毫秒

1KB=8比特×1024=8192比特

发送时间：1000KB÷1.5Mbps=8192000比特÷1500，000比特/秒=5.46秒

所以，总时间等于0.2+5.46+0.05=5.71秒。

（b）带宽是1.5Mbps，但在结束发送每一个数据分组之后，必须等待一个RTT才能发送下一个数据分组。

解答：在上一小题（a）答案的基础上再增加999个RTT

5.71+999×0.1=105.61秒

所以，总时间是105.61秒。

（c）带宽是无限大的值，即我们取发送时间为0，并且在等待每个RTT后可发送多达20个分组。

解答：1000KB÷1KB=1000分组　　1000分组÷20分组=50个RTT

50-1=49个RTT

2×RTT+49RTT+0.5RTT=51.5RTT=0.1×51.5=5.15秒。

（d）带宽是无限大的值，在紧接起始握手后我们可以发送一个分组，此后，在第一次等待RTT后可发送2^1个分组，在第二次等待RTT后可发送2^2个分组，。。。。，在第n次等待RTT后可发送2^n个分组。

解答：取n=9

$1+2+4+\ldots+2^9=2^{9+1}-1=1023$

这样我们就可以发送所有的1000个分组，而且在第9次等待RTT后只须发送。

（512-23）个分组就可以了。

2RTT+9RTT+0.5RTT=11.5RTT

0.1×11.5=1.15秒

即总的延迟是1.15秒。

2. 考虑一个最大距离为2公里的局域网，当带宽等于多大时传播延时（传播速度为2×10^8米/秒）等于100字节分组的发送延时？对于512字节分组结果又当如何？

解答：传播延迟等于：

2×10^3米÷（2×10^8米/秒）=10^{-5}秒=10微秒

100字节÷10微秒=10M字节/秒=80M位/秒

512字节÷10微秒=51.2M字节/秒=409.6M位/秒

因此，带宽应分别等于80M位/秒和409.6M位/秒。

3. 假定有一个通信协议，每个分组都引入100字节的开销用于头和成帧。现在使用这个协议发送1M字节的数据，然而在传送的过程中有一个字节被破坏了，因而包含该字节的那个分组被丢弃。试对于1000、5000、10000和20000字节的分组数据大小分别计算“开销+丢失”字节的总数目？分组数据大小的最佳值是多少？

解答：设D是分组数据的大小，那么所需要的分组数目 $N=10^6/D$

开销=100×N （被丢弃分组的头部也已计入开销）

所以，开销+丢失=$100\times10^6/D+D$

分组数据大小 D	开销+丢弃
1000	101000
5000	25000
10000	20000
20000	25000

$y=10^8/D+D$

$$\frac{dy}{dD}=1-\frac{10^8}{D^2}$$

当$D=10^4$时，

$\frac{dy}{dD}=0$所以，D的最佳值是10000字节。

4. 计算在下列情况下的延迟（从发出第1位开始到收到最后1位为止）：

（a）在通路上有1个存储转发交换机的10Mbps以太网，分组大小是5000位。假定每条链路引入10微妙的传播延迟，并且交换机在接收完分组之后立即重发。

解答：1位的发送延迟是0.1μs，一个分组由5000位组成，在每条链路上引入的发送延迟是500μs ，分组在每条链路上的传播延迟都是10μs，因此总的延迟等于：500×2+10×2=1020μs。

（b）跟（a）的情况类似，但有3个交换机。

解答：3个交换机，共有4条链路，总的延迟等于：

500×4+10×4=2040μs=2.04ms。

（c）跟（a）的情况相同，但假定交换机实施“直通”交换：它可以在收到分组的开头200位后就重发分组。

解答：使用直通交换，交换机延迟分组200位，即20μs。在这种情况下仍然有1个500μs的发送延迟，2个10μs的传播延迟，再加上20μs的交换机转发延迟，因此总的延迟等于：

500×1+10×2+20=540μs

如果像（b）那样有3个交换机，那么总的延迟将会等于：

500×1+10×4+20×3=600μs。

5. 计算在下列情况下的有效带宽。对于（a）和（b）假定有一个稳定的数据源供发送；对于（c）只要计算在12小时内的平均值即可。

（a）类似于A4-（b）10Mbps以太网通过了3个存储转发交换机，交换机在一条链路上接收的同时可以在另一条链路上发送。

解答：有效带宽是10Mbps。发送方可以用这个速率稳定地发送数据，交换机只是沿着流水线对数据进行流传送。在这里我们假定不发送ACKs，交换机能够保持和缓冲至少1个分组。

（b）跟（a）中的情况相同，但发送方在发送每个5000位数据分组后必须等待一个50字节的确认分组。

解答：在发送方向上的延迟累计为500×4+10×4=2040μs=2.04ms。在每条链路上的ACK延迟有对于400位的发送延迟40μs和传播延迟10μs，所以在ACK方向上的延迟累计为40×4+10×4=200μs=0.2ms。总的RTT等于2.04+0.2=2.24ms。

因此有效带宽等于5000位÷2.24毫秒=2.2Mbps。

（c）夜间（12小时）船运100张CD盘（每个盘650MB）

解答：$100\times6.5\times10^{8}$字节/12小时 $=6.5\times10^{10}$字节/（12×3600秒）= 1.5M字节/秒 ＝12M

位/秒。

6. 在下列情况下，假定没有数据压缩，对于（a）-（c）试计算实时传送所需要的带宽。

（a）分辨率为640×480的视频，每个像素3个字节，每秒30帧。

解答：640×480×3×30=26.4M字节/秒 （$1M=1024^2$）

（b）160×120视频，每个像素1字节，每秒5帧

解答：160×120×1×5=96000字节/秒=94KB/s （1KB=1024字节）

（c）CD-ROM音乐，1张CD可以放75分钟，容量为650MB

解答：650MB/75分=8.7MB/分=148KB/秒 （1K=1024）

（d）假定传真发送一幅8×10英尺的黑白图像，分辨率为每英寸72个像素。在14.4kbps的Modem上这要花多长时间？

解答：8×10×72×72=414720位=51840字节

414720位÷14400位/秒=28.8秒

7. 假定一个共享媒体M以轮转的方式提供机会给主机A1、A2、……AN发送一个分组，没有数据要发送的主机立即放弃M。这跟同步时分多路复用（STDM）有什么不同？跟STDM相比，采用这个方案的网络利用率如何？

解答：在STDM中，所提供的时间片总是相同长度，如果不被所分配给的站使用，就会造成浪费。本题中的轮转访问机制给每个站发送一个分组的机会，在一定的最大分组长度限制范围内，分组可长可短，因此各个站的发送时间并不相同，可以根据需要改变，没有数据要发送的站可以不占用发送时间。正因为如此，该访问机制的网络利用率可能高得多。

8. 考虑在一条链路上传送文件的一个简单协议。在经过某种初始的协商之后，A给B发送1KB大小的数据分组，B然后用一个确认应答。A在发送下一个数据分组之前总是要等待前一个ACK（确认），这就是通常所说的停-等协议。在一个预定的时间内未收到确认的分组，就认为是丢失了，并且进行重发送。

（a）在不会有分组丢失或重复的情况下，说明为什么在分组头中包含“序列号”是不必要的？

解答：在不会有分组丢失或接收重复分组的情况下，当我们期待接收第N个分组时，就一定接收到第N 个分组，因此我们可以在接收方本地保持跟踪分组的顺序号N。

（b）假定链路可能偶尔地丢失分组，但分组总是以发送的顺序到达接收方。为了让A和B能够检测到和重发丢失的分组，使用2位做序列号够用吗？1位怎么样？

解答：为了能够区分所收到的是一个新的分组，还是前一个分组的重复拷贝，需要至少1位序列号。

（c）现在假定链路可能投递无序，有时候1个分组投递可能花1分钟时间，在若干后随分组之后到达。这会怎样改变对序列号的需求？

解答：对于允许的失序投递，长至1分钟时间的多个分组必须通过顺序号区别开来。否则一个很老的分组可能到达时被作为当前分组接收。序列号的个数必须多至：

带宽×1分钟/分组大小。

9. 影响一个“存储-转发”式分组交换系统的延迟的一个因素是通过交换机存储转发一个分组要花多长时间。假定在铜线和光纤中的传播速度是光在真空中的速度的2/3，并假定客户机在纽约，服务器在加利福尼亚。如果交换时间是10微秒，那么它可能是影响这个“客户-服务器”系统的响应时间的主要因素吗？

解答：不是。传播速度是200，000公里/秒或200米/微秒。在10微秒的时间内，信号传播2公里。因此每个交换机加进相当于2公里额外线缆的延迟。如果客户机和服务器相隔5000公里，即使跨越50个交换机，也仅相当于在总的通路上加进100公里的额外线缆，只是5000公里的2%。因此，在这种情况下交换延迟不是影响响应时间的主要因素。

10. 在未来，当每个人都有一个家庭终端连到计算机网络时，对重要的未决立法的公众即时表决将成为可能。最终，现有的立法机构可能消亡，让民众的意愿直接地表达出来。这种直接民主的正面方面是很显然的，试讨论它的一些负面方面。

解答：这里很显然没有单个正确的答案，但下列几点看来是相关的。现在的系统在其机制中有大量的惯性(检查和平衡).这种惯性在每次不同派别轮换执政时可能有助于已有的立法的、经济的和社会的系统不被推翻。而且，有许多人对争论的社会问题持有强烈的观点，但他们并不真正了解事实的真相，允许理由不充分的观点写进法律是不合适的。这种或那种特别利益组织大做广告的潜在影响也必须予以考虑。另一个重要影响是安全性，许多人可能担心一些青少年攻击系统，并篡改结果。

11. 一幅图像有1024×768个像素，每个像素3个字节。假定该图像不压缩。在一个56kbps的Modem上要花多长时间？在1Mbps的电缆Modem上要花多长时间？在10Mbps的以太网上要花多长时间？在100Mbps的以太网上呢？

解答：该图像的数据量是1024×768×3即2，359，296字节，即18，874，368位。

在56，000位/秒 速率下，要花337.042秒；
在1M位/秒速率下，要花18.874秒；
在10M位/秒 速率下，要花1.887秒；
在100M位/秒 速率下，要花0.189秒。

12. 假定有一个人训练他的小狗为他运送一个包含3盘8毫米磁带的盒子。每一盘磁带的容量都是7千兆字节，小狗以每小时18公里的速度向你跑来。问在什么样的距离范围内，小狗的数据传输速率要高于150Mbps的传输线路的传输速率？

解答：狗可以运载21千兆字节，即168千兆位。每小时18公里的速度等于每秒0.005公

里，跑x公里花费的时间是x/0.005=200x秒，所产生的运载数据的速率等于

[168 /（200x）]Gbps，即840/x Mbps.

令840/x>150, 得到 x<5.6公里

因此在小于5.6公里的距离范围内，小狗的数据传输速率比150Mbps的传输线路高。

13. 特种漆公司的总裁有了一个想法，要跟本地的一个啤酒酿造商一起生产一种不显眼的啤酒罐头盒（作为一种防止乱丢垃圾影响市容的措施）。总裁让他的法律部门研究这件事，法律部门又请工程部门帮助。结果，总工程师打电话给对方公司的相应人员讨论项目的技术方面。然后双方的工程师向各自的法律部门报告，后者又通过电话协商安排法律方面的事项。最后，两个公司的总裁讨论该交易的财务方面的问题。在OSI模型的意义上，这是一个多层协议的例子吗？

解答：不是。在ISO的协议模型中，物理通信仅发生在最底层，而不是在每一层都发生。

14. 图1-5示出了一种服务。在该图中是否隐含着其它的服务？如果是，在哪里？如果否，为什么？

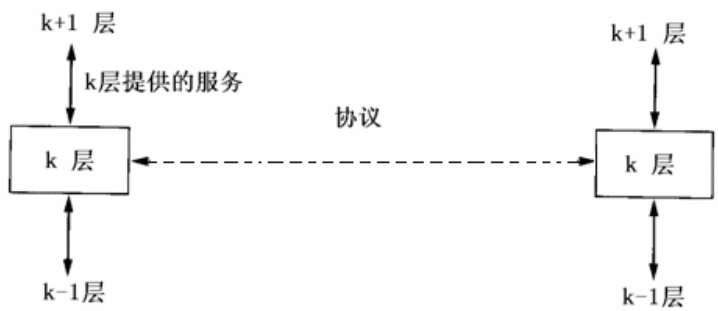


图 1-5　服务和协议之间的关系

解答：图中所示的服务是k层向k+1层提供的服务。另一个一定存在的服务是在k层下面，该服务由下面的k−1层向k层提供。

15. 如果在数据链路级交换的单元叫做帧，在网络级交换的单元叫做分组，那么是帧封装分组，还是分组封装帧？请解释你的答案。

解答：是帧封装分组。当一个分组到达数据链路层时，整个分组，包括头和数据，都被用作一个帧的数据域。这就好像把整个分组放在一个信封内，因此我们说是帧封装分组。

16. 当系统中既有固定部分也有可移动部分时，例如软盘驱动器和软盘，对该系统进行标准化是很重要的。这样不同的公司就都可以制造固定部分和可移动部分，并且它们可以组合在一起工作。举出在计算机工业之外存在这种国际标准的3个例子。再给出在计算机工业之外不存在这种国际标准的3个领域。

解答：具有国际标准的系统的例子包括CD播放器和它们的盘，随身听和录音磁带，照相机和35毫米胶卷，自动出纳机和银行卡片。缺乏国际标准的领域包括盒式录象机和录象

带（在美国是NTSC VHS，在欧洲是PAL，在其它国家还有SECAM VHS），手提电话，电灯和灯泡（不同的国家使用不同的电压），影印机和纸（在美国是8.5x11英寸，其它地方是A4），螺钉和螺母（英制和公制螺距）。

17. 举出网络协议建立国际标准的两个优点和两个缺点。

解答：一个优点是如果每个人都使用标准，那么每一个人都可以跟其他任何人交流。另一个优点是广泛使用标准将导致规模经济，比如生产大规模集成电路芯片。

一个缺点是为了取得标准化所需要的政治妥协经常导致差的标准。另一个缺点是一旦标准被广泛采用了，要对它进行改变就会非常困难，即使发现了新的和更好的技术或方法，也难以替换。另外，标准化的过程需要一段时间，当标准被接受的时候，它可能已经是过时的了。

18. 在FM（调频）电台广播中，SAP（服务访问点）地址是什么？

解答：SAP（服务访问点）地址是所使用的频率，例如87.6、103.9等。

19. 无连接通信和面向连接的通信之间的主要区别是什么？

解答：面向连接的通信有三个阶段。在连接建立阶段，先要做一个请求，然后才能建立连接。仅仅在这个阶段被成功地完成后，才可以开始数据传送阶段。然后是连接释放阶段。无连接通信没有这些阶段。它只是发送数据。

20. 有两个网络，它们都提供可靠的面向连接的服务。一个提供可靠的字节流，另一个提供可靠的报文流。请问二者是否相同？为什么？

解答：不相同。在报文流中，网络保持对报文边界的跟踪；而在字节流中，网络不做这样的跟踪。例如，一个进程向一条连接写了1024字节，稍后又写了另外1024字节。那么接收方共读了2048字节。对于报文流，接收方将得到两个报文，每个报文1024字节。而对于字节流，报文边界不被识别。接收方把全部的2048字节当作一个整体，在此已经体现不出原先有两个不同的报文的事实。

21. 在两台计算机之间传输一个文件，有两种可行的确认策略。第一种策略把文件截成分组，接收方逐个地确认分组，但就整体而言，文件的传送没有得到确认。第二种策略不确认单个分组，但当文件全部收到后，对整个文件予以接收确认。请讨论这两种方式的优缺点。

解答：如果网络容易丢失分组，那么对每个分组逐一进行确认较好，此时仅重传丢失的分组。而在另一方面，如果网络高度可靠，那么在不发生差错的情况下，仅在整个文件传送的结尾发送一次确认，从而减少了确认的次数，节省了带宽；不过，即使有单个分组丢失，也需要重传整个文件。

22. 当讨论网络协议时，“协商”的含义是什么？请举出一个例子。

解答：协商是要让双方就在通信期间将使用的某些参数或值达成一致。最大分组长度就是一个例子。

23. 在OSI模型中，是TPDU（运输层协议数据单元）封装网络层分组，还是网络层分组封装TPDU？请讨论。

解答：网络层分组封装TPDU。当TPDU向下到达网络层的时候，整个TPDU，包括其头和数据，都被用作网络层分组的数据段。也就是说，整个TPDU都被放到一个信封中。

24. 列举OSI参考模型和TCP/IP参考模型相同的两个方面。再列举它们不同的两个方面。

解答：相同的两个方面：

- 两个模型都是基于分层协议。两者都有网络层、运输层和应用层。
- 在两个模型中，运输服务都可以提供可靠的端到端的字节流。
  但它们在多个方面是不同的。
- TCP/IP没有会话层，也没有表示层。
- OSI不支持网络互连；OSI在网络层既有无连接服务，也有面向连接的服务。

25. 图1-6示出的网络的设计是要经受得住核战争。假定任意一颗炸弹消灭一个节点以及所有跟它连接的链路，那么，需要多少颗炸弹才能把所有的节点划分成互相隔离的两个部分？

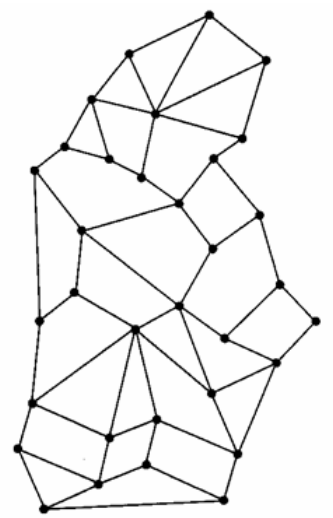


图 1-6　一个分布式交换系统

解答：使用3颗炸弹可以把右上角的两个节点跟其余节点隔离开来。3颗炸弹除掉了这两个节点所连接的3个节点。事实上，该系统可以承受任意两个节点的丢失。

26. 因特网的规模大约每18个月翻一番，虽然无人能肯定，但有人估计在2001年因特网上的主机数已达到1亿台。请根据这些数据计算到2010年时因特网上预估的主机数。你相信这个数字吗？请解释你的回答。

解答：每18个月翻一番，意味着3年增加到4倍，那么9年将增加到4^3即64倍，导致64亿

台主机。

也许这种计算过于保守，因为到了2010年，也许世界上的每一台电视机以及数十亿的其它电器都将在局域网上，并连接到因特网。那时候，在发达世界中的普通人都可能有数十台因特网主机。

27. TCP和UDP之间的主要区别是什么？

解答：TCP是面向连接的，而UDP是一种数据报服务。

28. 有5个路由器要连成一个点到点结构的子网。在每一对路由器之间可以设置一条高速线路，或者是一条中速线路，或者是一条低速线路，也可以不设置任何线路。如果产生和考察每一种拓扑要花100毫秒的计算机时间，那么为了寻找匹配预期负载的拓扑而考察所有可能的拓扑需用多长时间？

解答：设这5个路由器分别叫做A、B、C、D和E。存在10条可能的线路：AB、AC、AD、AE、BC、BD、BE、CD、CE和DE。它们中的每一条都有4种可能性：3种速率以及没有线路；因此总的拓扑数等于4^{10}=1048576。因为每种拓扑花100毫秒的时间，所以总共需用的时间等于104857.6秒，即约为29小时。

29. 参照图1-7回答问题。图中的每个方框表示一个网络节点。以星号标注的圆圈表示你的终端。

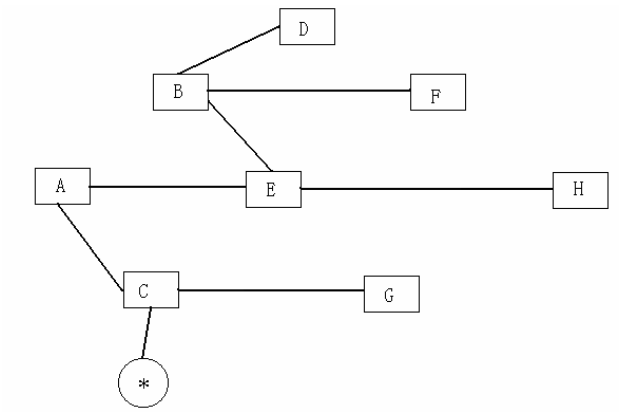


图 1-7　习题 29 插图

（a）你的本地节点是哪一个节点？

答：C

（b）哪些节点是你的本地节点的相邻节点？

答：A和G

（c）对你的本地节点来说，哪些节点是远程节点？

答：A、B、D、E、F、G和H

（d）哪些节点是终端节点（END NODES）？

答：D、F、G和H

（e）哪些节点是路由节点（ROUTING NODES）？

答：A、B、C和E

（f）从节点F到G的最短通路有多少个跳段（HOPS）？

答：5

30. 在ISO/OSI参考模型中，同层对等实体间进行信息交换时必须遵守的规则为（A），相邻层间进行信息交换时必须遵守的规则称为（B），相邻层间进行信息交换时使用的一组操作原语称为（C）。（D）层的主要功能是提供端到端的信息传送，它利用（E）层提供的服务完成此功能。

可供选择的答案：

A、B、C：1.接口；2.协议；3.服务；4.关系；5.调用；6.连接。
D、E：1.表示；2.数据链路；3.网络；4.会话；5.运输；6.应用。

答题填空：A(　　); B(　　); C(　　); D(　　)；E(　　)

解答：A(2.协议); B(1.接口); C(3.服务); D(5.运输)；E(3.网络)

31．计算机网络中，分层和协议的集合称为计算机网络的（A）。其中，实际应用最广泛的(A)是（B），由它组成了(C)的一整套协议。

可供选择的答案：

A：1组成结构；2参考模型；3体系结构；4基本功能。
B：1.SNA；2.MAP/TOP；3.TCP/IP；4.X.25；5.ISO/OSI。
C：1.ISO/OSI网；2.局域网；3.Internet；4.分组交换网

答题填空：A(　　); B(　　); C(　　)。

解答：A(3体系结构); B(3.TCP/IP); C(3.Internet)。

32．名词解释

网络服务质量QoS; QoS特性参数。

解答：服务质量（QoS）是指为保证所提供服务的质量达到相应标准而采取的一系列措施的技术总称。网络对不同应用的分组有不同的处理方式。人们把可以提供这些不同级别的服务的网络称作是支持QoS（服务质量）的网络。

QoS特性参数重点有三个方面，一是带宽和用户可得到的速率，二是延迟，三是延迟变化；当然，传统的误码率和可靠性指标，还有越来越显得重要的安全性也是不可忽视的。

33．写出基本的运输服务原语组（运输连接建立、释放和数据传输各原语组）。试用

状态转换图，画出在一个运输连接上的这些运输服务原语有效时序关系。

解答：T_CONNECT.request,　　T_CONNECT.indication,
T_CONNECT.response,　　T_CONNECT.confirm,
T_DISCONNECT.request,　　T_DISCONNECT.indication,
T_DATA.request,　　T_DATA.indication,
T_EXPEDITED_ DATA.request,　T_EXPEDITED_ DATA.indication。

图1-8画出了在一个运输连接上的这些运输服务原语的有效时序关系。

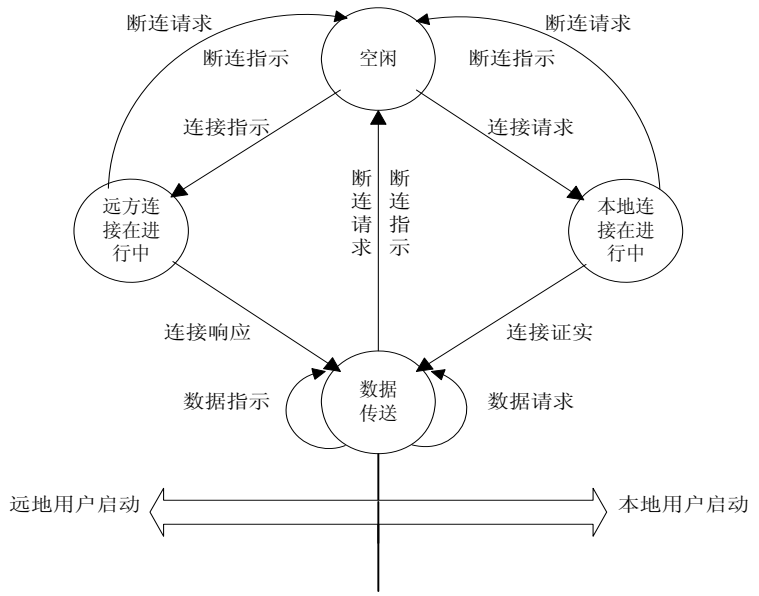


图 1-8　在一个运输连接上运输服务原语的有效时序关系

第 2 章　物 理 层

本章学习重点

- 傅里叶分析和有限带宽信号
- 信道的最大数据传输率
- 传输媒体
- 数据编码技术
- 多路复用技术
- 电话线路及相关的数字化技术

2.1　基本知识点

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的比特流，而不是指连接计算机的具体的物理设备或具体的传输媒体。现有的计算机网络中的物理设备和传输媒体的种类非常繁多，而通信手段也有许多不同的方式。物理层的作用正是要尽可能地屏蔽掉这些差异，使其上面的数据链路层感觉不到这些差异。

在物理连接上的传输方式一般都是串行传输，即一个一个比特按照时间顺序传输。当然在某些情况下也可以采用多个比特的并行传输方式。出于经济上的考虑，远距离的传输通常都是串行传输。

物理层是OSI 模型的最低层，涉及网络物理设备之间的接口，其目的是向高层提供透明的二进制位流传输。物理接口的设计涉及信号电平、信号宽度、传送方式（半双工或全双工）、物理连接的建立和拆除、接插件引脚的规格和作用等。总之，物理层提供为建立、维护和拆除物理链路所需的机械、电气、功能和过程特征。

2.1.1　数据传输的基础知识

表示成时间的函数，电磁信号可以是连续的，也可以是离散的。连续信号的强度随时间平滑变化，也就是说，在信号中无断裂或不连续。离散信号的强度在某个时间周期内维持一个常量级，然后改变到另一个常量级。连续信号可以表示语音，离散信号可以表示二进制的1和0。最简单的信号种类是周期信号，同样的信号模式随时间反复出现。

19世纪初叶，法国数学家吉·傅里叶证明：任何正常的周期为T的函数g(t)都可以由无限个正弦和余弦函数合成。一个持续时间有限的数据信号可以想象成它一遍又一遍地无限重复整个模式，即假定从T到2T的区间模式等同于区间0到T，从2T到3T的区间模式又等同于区间T到2T，如此等等。

所有传输设施在传输信号过程中都将损失一些能量。如果所有傅里叶分量被等量衰减，那么结果信号虽在振幅上有所衰减，但没有畸变。然而，实际的传输设施对不同的傅里叶分量衰减程度不同，因而输出信号发生畸变，通常频率0到fc(截止频率，以赫兹即Hz为单位)范围内的谐波在传输过程中无衰减，而截止频率以上的所有谐波在传输过程中衰减极大。这种现象既可由传输媒体的物理特性引起，也可能是由于人们有意在线路中安装了一个滤波器来限制每个用户使用的带宽。

普通的电话线路常称话音级线路，截止频率大约为3000Hz，这就意味着允许通过的最高简单正弦或余弦周期信号的频率是3000Hz。

早在1924年，奈魁斯特(Nyguist, H)就认识到信道对于数据传输率的限制，并推导出了一个有限带宽无噪声信道的最大数据传输率表达式。奈魁斯特证明，如果一个任意的信号通过带宽为H的低通滤波器，那么每秒采样2H次就能完整地重现通过这个滤波器的信号。以每秒高于2H次的速度对此线路采样是无意义的，因为高频的分量已被滤波器滤掉，无法再恢复了。如果被传信号电平分为V级，奈氏定理表明：最大数据传输率=2HlbV(bit/s)。例如，一个无噪声的3KHz信道不能以高于6000bit/s的速率传输二元(即两级)电平信号。

如果有噪声存在，情形会急剧变坏。噪声通常以信号功率和噪声功率之比来度量，这个比值叫做信噪比。如果用S表示信号功率，N表示噪声功率，则信噪比为S/N。通常，我们并不使用信噪比本身，而是使用10lg S/N，其单位为分贝(dB)，如果S/N为10，则是10dB，S/N为100则是20dB，S/N为1000是30dB，依此类推。

1948年，仙农(Shannon, C. E)把奈魁斯特的结论进一步扩展到受随机(热)噪声影响的信号。他的关于噪音信道的主要结论是：对任何带宽为H 赫兹、信噪比为S/N的信道：

$$\text{最大数据传输率（bit）} = H\log_2(1+\frac{S}{N})$$

仙农公式表明，信道的带宽越大或信道中的信噪比越大，则信息的极限传输速率就越高。从仙农公式可看出，若信道带宽H或信噪比S/W没有上限（实际的信道当然不可能是这样的），那么信道的极限信息传输速率也就没有上限。仙农的结论是应用信息论原理推导出来的，适用范围很广。要想超越这一结论可以认为想要发明永动机。应该注意的是，这是一个上限。实际上要接近仙农极限也是很困难的。

自从仙农公式发表以后，各种新的信号处理和调制的方法不断出现，其目的都是为了接近仙农公式所给出的传输速率极限。在实际信道上能够达到的信息传输速率要比仙农的极限传输速率低不少。这是因为在实际的信道中，信号还要受到其他的一些损伤，如各种系统外的噪声干扰以及在传输和处理中产生的其他失真等。这些因素在仙农公式的推导过程中并未考虑。

由于波特率受奈氏准则的制约，所以要提高信息的传输速率，就必须设法使每一个信号码元能携带更多个比特的信息量。这就需要采用多元制的调制方法。例如，当采用16元制时，一个码元可携带4个比特的信息。一个标准电话话路的频带为300~3400Hz，即带宽为3100Hz。在这频带中接近理想信道的也就是靠中间的一段，其带宽约为2400Hz左右。如使信号的传输速率为2400波特，通过4位/波特调制，则信息的传输速率可达到9600bit/s。从仙农公式可以很容易地计算出在这种情况下所需信噪比的最低值。但应注意，对于实际的信道所需的信噪比要比这个最低值还要高不少。

对于3.1kHz带宽的标准电话信道，如果信噪比S/N=2500，那么由仙农公式可以知道，无论采用何种先进的编码技术，信息的传输速率一定不可能超过由仙农公式算出的极限数值，即35000bit/s左右。目前的编码技术水平与此极限数值相比，差距已经很小了。

2.1.2 传输媒体

传输介质是在数据传输系统中位于发送设备和接收设备之间的物理通路。数据传输的特征和质量是由介质的特征和信号的特征两个方面决定的。在导线介质的情况下，介质本身在确定传输限制方面起更重要的作用。对于非导线介质，由发射天线产生的信号带宽在确定传输特征方面比介质更为重要。由天线发射的信号的一个关键特性是方向性。一般说来，低频信号是全向的，亦即从天线发出的信号在所有的方向上传播。在高频的发射中，信号可以被集中到一个定向的射束。

在现实的世界中，有多种物理介质可用于实际的传输，每一种物理介质在带宽、延迟、成本和安装维护难度上都不相同。

无论是传输模拟数据还是传输数字数据，最普通的传输介质是双绞线。双绞线由两条互相绝缘的铜线组成，其典型粗细为直径1mm，这两条线像螺纹一样拧在一起，这样可以减少邻近线路的电气干扰。双绞线最常见的应用是电话系统。几乎所有的电话都通过双绞线连接到电话局。双绞线传输信号可以几公里不需要放大，更远的距离就要使用中继设备了。当有许多双绞线并行走线太长时，例如在一座公寓里连往电话局的所有导线应扎成束，并包封在护套中。在电话线架设在地面电线杆子上的地区，常常可以看到直径为几厘米的线束。

双绞线的带宽取决于铜线的粗细和传输距离，但在许多情况下，几公里范围内的传输速率可以达到几兆bps，由于其性能较好又价格便宜，双绞线很有可能还要被持续使用多年。

双绞线可以分为两种：非屏蔽和屏蔽。非屏蔽双绞线电缆由多对双绞线和一个塑料外皮构成。非屏蔽双绞线（UTP）易受外部干扰，包括来自环境噪音与附近的双绞线；但由于其价格低廉且易于安装和使用，所以应用非常广泛。在建筑物内部，作为局域网传输介质而被普遍使用的UTP电缆的最大长度一般限制在100米之内。

屏蔽双绞线电缆的内部与非屏蔽双绞线电缆一样是双绞铜线，外层由铝箔包着。屏蔽双绞线（STP）在抗干扰方面优于UTP，但它相对来讲要贵一些，并且需要配有支持屏蔽功能的特殊连接器和相应的安装技术。屏蔽双绞线在低速时提供良好的性能。屏蔽双绞线除了用于IBM网络产品安装（主要采用16Mbps速率）外，并未普遍流行起来。

1991年，美国电子工业协会（EIA）颁布了EIA-568标准，即商业大楼的通信布线标准。EIA-568-A有三种UTP电缆。

3类：UTP电缆及其端接设备的传输特性定义为16MHz。

4类：UTP电缆及其端接设备的传输特性定义为20MHz。

5类：UTP电缆及其端接设备的传输特性定义为100MHz。

3类UTP电缆对应于在大多数办公楼里大量使用的话音级电缆；在有限的距离内，经过适当的设计，数据速率可以达到16Mbps。

5类是数字级电缆，现正成为新建大楼的预装设施；在一定的范围内，经过适当的设计，

5类电缆可以达到100Mbps速率。

3类和5类UTP的关键差别在于单位距离上的螺旋的数目。5类旋得较紧，一般为每英寸3-4转，而3类则一般是每英尺3-4转；旋得越紧，价格越贵，但性能也好得多。

同轴电缆由绕同一轴线的两个导体所组成。它以硬铜线为芯，外裹一层绝缘材料，这层绝缘体外面又被密集的网状导体所环绕，网外又覆盖一个保护性塑料层。同轴电缆的这种结构，使它具有比双绞线更好的抗干扰性能。它可以传输比双绞线更长的距离，连接更多的工作站。同轴电缆的带宽取决于电缆长度，1km的电缆可以达到1Gb/s至2Gb/s的数据传输速率。同轴电缆曾在电路系统中广泛使用，现在已大量被光纤所代替。但是，现在同轴电缆仍被广泛地用于有线电视和某些局域网。

有两种广泛使用的同轴电缆。一种是50Ω电缆，用于基带数字传输，另一种是75Ω电缆，用于宽带模拟传输。“宽带”这个词来源于电话业，指比4KHz宽的频带；然而在计算机网络中，“宽带电缆”是指使用模拟信号传输数字数据的较宽频带的电缆。

基带电缆使用数字信号，在这种情况下，信号占据整个频宽，电缆上只有一个信道。基带电缆主要用于局域以太网，并使用曼彻斯特编码，数据速率一般是10Mbps。宽带电缆使用标准的有线电视技术，频带可高达300——450MHz。由于使用模拟信号，传输距离可以达到100公里。为了在模拟网上传输数字信号，需要在接口处安放一个电子设备，用以把进入网络的比特流转换为模拟信号，并把网络输出的信号再转换成比特流。取决于这些电子设备的类型，1bps占据大约1Hz的带宽。使用先进的调制技术，可以达到每赫兹多个比特。宽带系统又分为多个信道，电视广播通常占用6MHz信道。每个信道可用于模拟电视、CD质量声音(1.4Mb/s)或3Mb/s的数字比特流。电视和数据可在一条电缆上混合传输。

宽带系统有很多种使用方式。在一对计算机之间可以分配专用的永久性信道；另一些计算机可以通过控制信道申请建立一个临时连接，然后切换到申请得到的信道；还可以让所有的计算机竞争访问单个信道或一组信道。从技术上讲，宽带电缆在传送数字数据方面要比基带（即单一信道）电缆差，但它的优点是已被广泛安装。面对电话公司和有线电视公司激烈竞争的形势，我们可以预期有线电视系统会作为计算机城域网运行，并会越来越多地在它上面提供电话和其它服务。

由于光技术的发展，我们已经可以利用光脉冲来传输数据。光脉冲的出现表示其位为1，不出现表示为0。可见光的频率大约是1014Hz，因而光传输系统可使用的带宽范围极大。

光导纤维是一种能够传导光信号的极细而柔软的通信介质，有许多种玻璃和塑料可用来制造光导纤维。光导纤维的横截面为圆形，由纤芯和包层两部分构成。二者由两种光学性能不同的介质构成。其中，纤芯为光通路；包层由多层反射玻璃纤维构成，用来将光线反射到纤芯上。实用的光缆外部还须有一个保护层，每一芯及包层或紧或松地被外壳包裹着。在紧型结构中，光纤被外层塑料壳完全包住；在松型结构中，光纤与保护壳之间有一层液体胶或其他材料。无论哪一种结构，外壳都是起着提供必要的光缆强度的作用，以防止光纤受外界温度、弯曲、外拉、折断等影响。可将多股光纤捆在一起放在光缆中心。光纤要比铜导线细得多，也轻得多，所以大型光缆能够比同尺寸的铜电缆具有更高的吞吐率。这一特点使光纤在空间有限的环境下使用更理想。

光纤是利用全内反射来传输经信号编码的光束。全内反射可出现在折射率大于周围媒体的折射率的任意透明媒体中。来自光源的光进入圆柱形玻璃或塑料纤芯。当纤芯半径较

大时，大角度的入射光线被反射并沿光纤传播，其余光线被周围媒体所吸收。这种传播方式因有多个反射角而被称为多模方式。当纤芯半径减小时，被反射的角度亦加大。当将纤芯半径降低到波长的量级时，只有单个角度即只有轴向光束能通过，此时光纤如同一个波导，称为单模光纤。

在多模传输时，存在多个传输路径，每一路径的长度不同，因此越过光纤的时间不同。这使信号码元在时间上出现扩散，限制了能准确接收的数据速率。由于单模传输时只存在单个传输途径，因此不会出现这种失真。另外，通过改变纤芯的折射率，还可以形成第三传输方式，称作梯度折射率多模方式。这种方式的特性介于普通多模与单模之间。

单模光纤具有更大的容量，但是它的生产要比多模光纤昂贵。光纤的类型由模、材料（玻璃或塑料纤维）及芯和外层尺寸所决定，芯的尺寸及纯度决定了光的传输量。当前最常使用的是62.5μm芯 /125μm外层的多模光纤，其次是的8.3μm芯 /125μm外层的单模光纤。光缆在普通计算机网络上的安装是从用户设备开始的。由于每根光纤在任何时候都只能单向传输，因此，要实行双向通信，它必须成对出现，一个用于输入，一个用于输出，光纤两端接到光学接口上。每一条光纤线缆的连接都需要小心地磨光端头，通过电烧烤或化学环氯工艺与光学接口连在一起。

光纤的传输距离仅受波长的影响，它的衰减率极低。同时为了更有效地增大传输距离，一般都采用1.55m波长的光纤，同时利用掺饵光纤放大器做为接收机的前置放大器或在光纤线路中作为中继器，可使光纤的传输距离为几十公里，甚至上百公里。由于光纤采用的是光谱技术，它没有泄漏信号的现象，也不受电磁波和高频失真的影响，这些特点使它更适合有危险的、高压的或者泄漏信号、干扰信号很强的环境。

无线传输介质都不需要架设或铺埋电缆或光纤，而通过大气传输,人们现在已经利用了无线电、微波、红外线和激光进行通信。无线通信已广泛应用于电话的领域，构成蜂窝式无线电话网，由于便携式计算机的出现以及在军事、野外等特殊场合下，移动式通信连网的需要促进了数字化无线移动通信的发展。现在已经有了无线局域网产品，能在一幢楼内提供快速、高性能的计算机连网技术。

微波通信的载波频率为2 — 40 GHz范围，因为频率很高，可同时传送大量信息，如一个带宽为2MHz的频段可容纳500条话音线路，用来传输数字信号，可达若干M bps。微波通信的工作频率很高，与通常的无线电波不一样，是沿直线传播的，由于地球表面是曲面，微波在地面的传播距离有限。直线传播的距离与天线的高度有关，天线越高距离越远，但超过一定的距离后就要用中继站来接力。

另外两种无线通信技术，红外通信和激光通信也像微波通信一样，有很强的方向性，都是沿直线传播的。

目前高带宽的计算机通信主要使用三种技术：微波，红外线和激光。这三种技术都需要在发送方和接收方之间有一条视线（line-of-sight）通路，有时统称这三者为视线介质。所不同的是红外通信和激光通信把要传输的信号分别转换为红外光信号和激光信号，再直接在空间传播。这三种视线介质由于都不需要铺设电缆，对于连接不同建筑物内的局域网特别有用。这是因为很难在建筑物之间架设电缆，不论在地下或用电线杆，特别是要穿越属于公共场所，例如要跨越公路时，会更加困难。而使用无线技术只需在每个建筑物顶上安装设备。这三种技术对环境气候较为敏感，例如，雨、雾和雷电。相对来说，微波对一

般雨和雾的敏感度较低。

卫星通信是微波通信中的一种特殊形式。卫星通信利用地球同步卫星作中继来转发微波信号，卫星通信可以克服地面微波通信距离的限制。一个同步卫星可以覆盖地球的三分之一以上表面，三个这样的卫星可以覆盖地球上全部通信区域，这样，地球上的各个地面站之间都可以互相通信了。由于卫星信道频带宽，也可采用频分多路复用技术分为若干子信道，有些用于地面站向卫星发送（称为上行信道），有些用于由卫星向地面转发（称为下行信道）。卫星通信的优点是容量大，距离远；缺点是传播延迟时间长。从发送站通过卫星转发到接收站的传播延迟时间为270ms，且这个传播延迟时间是和两站点间的距离无关的。这相对于地面电缆传播延迟时间约6μs/km来说，特别对于近距离的站点，要相差几个数量级。

2.1.3 数据编码技术

数据和传送数据所采用的信号是两个完全不同的概念。信号是数据的具体表示形式，它和数据有一定关系，但又和数据不同。模拟数据可以用模拟信号传输，也可以用数字信号传输；同样，数字数据可以用数字信号传输，也可以用模拟信号传输。这样就构成了四种方式。在每一种方式中，数据信息所对应的具体传输信号状态称为数据信息编码。

在电话机和本地局交换机之间所传输的信号就是采用模拟信号传输模拟数据的编码方式。模拟的声音数据是加载到模拟的载波信号中传输的。无线语音广播是模拟信号传输模拟数据的另一个例子。有效的传输需要比较高的频率。对于无导线传播，传送基带信号几乎是不可能的，因为那将需要直径为好几公里长的天线。另外，调制有助于频分复用。

我们在使用调制解调器通过电话线路传输计算机数据时，两端的计算机（数字设备）只能输出和接收数字信号，而所连接的电话系统的本地回路只能传输模拟信号。模拟信号传输的基础是载波，是一个连续变化的信号。用于远距离计算机通信的模拟线路一般为频带传输线路，适于传输模拟信号而不能传输基带信号（原始的电脉冲信号），即不能传输近似于零频率的分量（直流分量）。因此必须将数字数据变换（调制过程）成模拟信号后才能发送（模拟信号传输数字数据）；在接收端须进行逆变换，从而恢复数字数据的原形（解调过程）。使用模拟信号传输数字数据，依信号调制的参数不同，基本上可将调制分为三种：幅度调制，频率调制和相位调制。

在数字信号传输数字数据的编码方式中，通信的源端和目的端所发出和接收的以及中间媒体所传输的都是跳变的数字信号。具体用什么样的数字信号表示0以及用什么样的数字信号表示1就是所谓的编码。编码的规则可以有多种，原则上只要能有效地把1和0区分开就行。常用的数字信号编码方案有不归零制、曼彻斯特编码、差分曼彻斯特编码和4B/5B编码等。

使用数字信号编码模拟数据最常见的例子是用于音频信号的脉码调制（PCM）。它主要包括三个步骤，即抽样、量化和编码。抽样是指在每隔固定长度的时间点上抽取模拟数据的瞬时值，作为从这一次抽样到下一次抽样之间该模拟数据的代表值。根据抽样定理，当抽样的频率大于或等于模拟数据的频带宽度（最高变化频率）的两倍时，所得的离散信号可以无失真地代表被抽样的模拟数据。量化则是把抽样取得的电平幅值按照一定的分级

标度转换为对应的数字值，并取整数。这样，把连续的电平幅值转换为离散的数字量。

编码把量化的结果转换为对应的二进制编码。在网络系统中，把模拟数据编码成数字信号发送；或者反过来，把接收到的数字信号解码，还原成模拟数据的装置称为编码解码器（CODEC）。

2.1.4 多路复用技术

在实际的计算机网络系统中，传输媒体的能力往往超过来自单一信息源的需求，为了有效地利用通信线路，希望一个信道能够同时传输多路信号。多路复用技术就是把许多信号在单一的传输线路上用单一的传输设备进行传输的技术。采用多路复用技术把多个信号组合在一条物理线缆上传输，在远距离传输时可大大节省线缆的安装和维护费用。

两种最常使用的多路复用技术是频分多路复用和时分多路复用。其中时分多路复用又可分为同步时分和异步时分两种。

在物理信道能提供比单路原始信号宽得多的带宽的情况下，我们就可以把该物理信道的总带宽分割成若干个和传输的单路信号带宽相同（或稍微宽一点）的子信道，每个子信道传输一路信号。这就是频分多路复用。多路的原始信号在频分复用前，首先要通过频谱搬移把各路信号的频谱搬移到物理信道的不同频谱段上，这可以通过在频率调制时采用不同的载波来实现。

若媒体能达到的位传输速率超过单一信号源所要求的数据传输率，就可采用时分多路复用（TDM）技术，就是将一条物理信道按时间分成若干时间片轮流地给多个信号源使用，每一时间片由复用的一个信号源占用，而不象频分多路复用（FDM）那样同一时间同时发送多路信号。同步时分多路复用是指时分方案中的时间片是分配好的，而且是固定不变的，轮流占用，而不管某个信息源是否真有信息要发送。这样，时间片与信息源是固定对应的，或者说，各种信息源的传输定时是同步的，故称为同步TDM。在接收端，根据时间片序号便可判断是哪一路信息，因而便可送往相应的目的地。

异步时分多路复用允许动态地分配传输媒体的时间片。这样便可大大减少时间片的浪费。当然，实现起来要比同步TDM困难一些。在接收端无法根据时间片的序号来断定接收的是哪一路信息源的信息，因此，需要在所传输的信息中带有相应的信息。

时分多路复用TDM并不局限于传输数字信号，也可以用来分时传输模拟信号。另外对于模拟信号，有时可把TDM和FDM结合起来一起使用，即：一个传输系统中，可以频分成许多子信道，每个子信道再利用时分多路复用来细分。在宽带局域网中可以用此技术，而对于数字信号，一般不用FDM，因为数字信号占用的频带很宽。

波分多路复用是在光信道上采用的一种频分多路复用的变种，只不过光复用采用的技术与设备不同于电复用。不同光纤上的光波信号通过无源的棱柱或衍射光栅复用到一根长距离传输的光纤上。无源的设备通常运行得更可靠。由于光波处于频谱的高频段，有很高的带宽，因而可以实现非常多路的波分复用。此外，利用光耦合器和可调的光滤波器还可以实现光交换，或将在一根光纤上输入的光信号向多根输出光纤上转发。目前的技术已可使输出光纤的条数达到上百的数量级。

2.1.5 电话线路及相关的数字化技术

通常，每部电话都有两条铜线直接连接到电话公司最近的端局，这段距离通常为1-10km，这种用户电话和端局的双线连接在电话话务术语中称为本地回路。当接到某个端局的电话用户呼叫同一端局的另一用户时，端局内的交换机在两个本地回路间建立起一个直接的电气连接，在整个通话过程中这个连接保持不变。

如果受呼电话在别的端局，建立连接的过程就不同了。每个端局有大量的外线引到附近的一个或多个交换中心，即长途局（toll office），也称汇接局（tandem office）；连接端局和长途局的线路叫做长途接续干线（toll connecting trunks）。如果主叫端局与被叫端局到同一长途局碰巧都有一条长途接续干线（双方相距较近时很容易出现这种情况），便在这个长途局中建立接续。

如果主叫与被叫双方没有一个共同的长途局，那么路径就要在层次结构中某个更高层建立起来。还有地区局和区域局，这些局形成网络，借助于这些局又把长途局连接起来。长途电话局、地区电话局、区域电话局之间的彼此通信是经过宽频带的长途局际干线实现的，不同类别的交换中心数和它们的拓朴（例如两个地区局可以有一条直接接续还是必须经过一个区域局）随不同国家而异，这主要取决于它们的电话密度。现在，本地回路用一对绝缘导线，在交换局之间用同轴电缆、微波,使用光纤的情况更是日益广泛，其主要原因是光纤拥有极大的带宽，可以用一束光纤取代许多铜电缆，缓解了电缆管道中严重拥塞的情况。

数字传输优于模拟传输。首先，它的误码率很低。模拟电路的放大器补偿信号在线路中的衰减，然而它们决不能做到准确补偿，特别是衰减随频率而变化。由于误码具有累加性，长途通话经过许多放大器后很可能会有相当大的畸变。相反，数字再生器能够将衰减了的输入信号准确地恢复到它原来的值，因为输入信号只可能有两个值0和1，故数字再生器不具有累加性误码。

数字传输的另一个优点是，声音、数字、音乐，甚至电视、传真或者视频电话之类的图像能被复用（混合在一起），这样就能更有效地利用设备。此外，利用已有线路就可能获得更高的数据传输率。

当连接到数字端局的一个电话用户打电话时，从他的本地回路出现的信号是普通的模拟信号，这个模拟信号在端局被编码解码器（coder）数字化，产生7比特或8比特组成的数码。从某种意义上说，编码解码器和调制解调器相反：后者将数字位串转换为被调制的模拟信号；前者将连续的模拟信号转化为数字位串。编码解码器每秒进行8000次抽样（125微秒/样本），根据奈魁斯特原理，这个抽样速率足以从4KHz的带宽中捕获所有的信息。这个技术叫脉码调制（Pulse Code Modulation）。

一个使用很广的方法是贝尔系统的T1载波。T1载波能处理复用在一起的24条话音信道。轮流对各信道的模拟信号进行周期性采样，模拟信号串就被输入到1个(而不是24个)编码解码器进行数字化，再将数字输出合成一串。24条信道轮流将其采样的8位数字插入输出串，其中7位是数据，1位是控制信号，从而每条信道获得7×8000即56kbit/s的数据传输和1×8000即8K的控制信号传输。1帧包含24×8=192比特和1个附加的帧位，这样每125微秒193比特，总的数据率为1.544Mbit/s，第193位用于帧同步，其出现模式为0101010101…。通常，

接收器不断检查此位以保证没有失步，如果失步，接受器能够扫寻这一模式重新获得同步。模拟用户根本不会产生这个位模式，因为这相当于一个4000Hz的正弦波，它会被滤掉。当然数字用户能够产生这个模式，但是出现的概率极小。

CCITT有一个2.048Mbit/s脉码调制载波的推荐标准。这个载波将32个8位数据样本组成1个125微秒的基本帧，30个信道用于传信息，2个信道用于传控制信号。每4帧为一组。提供64个控制信息位，一半用于与信道有关的控制信号，另一半用于帧同步或留给各国自己安排。除北美和日本外，2.048Mbit/s的载波得到广泛的使用。与基本载波情况一样，在怎样把基本载波复用到更宽频带的载波方面，同样没有达成协议。贝尔系统T2、T3和T4标准的传输率分别为6.312、44.736和274.176Mbit/s，而CCITT的推荐标准是8.848、34.304、139.264和565.148Mbit/s。

就基于光纤的高带宽网络而言，在美国有一个被称作SONET（同步光纤网）的物理层标准。SONET为在光纤网上的传输定义了一系列的带宽等级。SONET速率由51.840Mbps这一基本速率的整数倍构成，包括51.840Mbps的OC-1（Optical Carrier-1）、OC-3（155.520Mbps）和OC-12（622.08 Mbps）。系统开发人员现在瞄准的目标是投递1244.160 Mbps（OC-24）和2488.320 Mbps（OC-48）。新的SONET标准则是OC-192（大约10 Gbps）以及更高的级别。

SONET是一种同步系统，它由一个主时钟控制，精度约为10^{-9}。SONET的所有级别都使用字节交叉的多路复用，线路速率都是基本STS-1级（51.84Mbps）的整数倍，没有任何附加的开销（在所有级别上都是大约3.3%）。而T载波系统的情况则显然不是如此。当前最高的可能级别是STS-256（13.271Gbps）。

在美国之外，SONET概念用SDH（同步数字体系）来描述。该体系使用155.520Mbps的建筑块，而不是51.840Mbps的建筑块。表2-1示出了SONET/SDH的多路复用层次。

表2-1　SONET 和 SDH多路复用的速率

SONET		SDH	数据速率（Mbps）		
电子的	光的	光的	局间	SPE	用户
STS-1	OC-1		51.84	50.112	49.536
STS-3	OC-3	STM-1	155.52	150.336	148.608
STS-9	OC-9	STM-3	466.56	451.008	445.824
STS-12	OC-12	STM-4	622.08	601.344	594.432
STS-18	OC-18	STM-6	933.12	902.016	891.648
STS-24	OC-24	STM-8	1244.16	1202.688	1188.864
STS-36	OC-36	STM-12	1866.24	1804.032	1783.296
STS-48	OC-48	STM-16	2488.32	2405.376	2377.728

在SONET多路复用层次中定义了从STS-1到STS-48的速率，对应于STS-n的光纤线路被称作OC-n。SDH名字有所不同，而且它们是从OC-3开始，因为基于CCITT的系统没有接近51.84Mbps的速率。不过，对于适当的聚合带宽值，它们基本上是一致的。另外，当一条线路（例如OC-3）没有被多路复用，而仅从一个源传送数据时，在名字后面加上一个字母c

（表示串联）。因此OC-3表示由3条单独的OC-1线路组成的155.52Mbps线路，而OC-3c则表示从一个源来的155.52Mbps数据流。

RS-232-C是计算机通过电话网络通信时与调制解调器间的接口标准。相应的国际标准是CCITT(国际电报和电话咨询委员会)推荐的标准V.24；它与RS-232-C相似，只是在某些很少使用的电路上稍有不同。在这个标准中，终端或计算机被正式地叫做数据终端设备DTE（Data Terminal Equipment），调制解调器（modem）被正式地叫做数据电路端接设备DCE（Data Circuit-Terminating Equipment），有时也简称为数据装置（DATA SET）。

EIA RS-232-C关于机械特性的要求，规定使用DB-25插针和插孔，插孔用于DCE方面，插针用于DTE方面。RS-232-C关于电气信号特性的要求，规定逻辑“1”的电平为低于-3V，而逻辑“0”的电平为高于+3V。

在所有遵从RS-232标准的系统中，DTE只有在下列4个电路都处于逻辑0（控制功能为ON）的条件下才可能发送数据：

- 请求发送RTS（针4）
- 清送CTS（针5）
- 数据端接装置就绪DSR（针6）
- 数据终端就绪DTR（针20）

依赖于DTE和DCE通信软件的具体配置情况，RTS-CTS握手过程可以逐个字符地进行，也可以逐个数据块地进行。一个更高层协议（与物理层协议相比）决定怎样组成一个字符或一块数据。如果10位组成一个字符，那么基于字符的握手过程每发送10位都需要DTE声言一次RTS信号，并从DCE接收一个CTS信号。对于逐块发送的握手过程，DTE在传递每块数据的末尾，都要发送一个特别的传送结束（end of transmission）字符，并关闭（OFF）RTS。

2.2 基本练习题

1. 什么是基带传输和频带传输？

解答：简单说来，基带传输采用基带信号，频带传输使用宽带信号。所谓基带信号就是将数字信号1或0直接用两种不同的电压来表示，然后送到线路上去传输。而宽带信号则是将基带信号进行调制后的频分复用模拟信号。基带信号经调制后其频谱被搬移到较高的频率处。由于每一路基带信号的频谱被搬移到不同的频段，因此合在一起后不会互相干扰。这样做就可以在一条电路中同时传送许多路的数字信号，因而提高了线路的利用率。

2. 名词解释

多模光纤和单模光纤

解答：来自光源的光进入圆柱形玻璃或塑料纤芯。大角度的入射光线被反射并沿光纤传播，其余光线被周围媒体所吸收。这种传播方式因有多个反射角而被称作多模方式，所

采用的光纤称为多模光纤。光线在纤芯半径减小时被反射的角度亦加大。当将纤芯半径降低到波长的数量级时，只有单个角度即只有轴向光束能通过，此时光纤如同一个波导，称为单模光纤。在多模传输时，存在多个传输路径，每一路径的传输长度不同，因此越过光纤的时间不同。这使信号码元在时间上出现扩散，限制了能准确接收的数据速率。由于单模传输时只存在单个传输途径，因此不会出现这种失真。

3. 选择题

下列哪一种传输方式被用于计算机内部的数据传输？

a. 串行
b. 并行
c. 同步
d. 异步

解答：b

4. 选择题

在串行传输中，所有的数据字符的比特

a. 在多根导线上同时传输
b. 在同一根导线上同时传输
c. 在传输介质上一次传输一位
d. 以一组16位的形式在传输介质上传输

解答：c

5. 选择题

波特率等于

a. 每秒传输的比特
b. 每秒钟可能发生的信号变化的次数
c. 每秒传输的周期数
d. 每秒传输的字节数

解答：b

6. 填空

当多个通信设备共享某个信道时，最常用的两种复用方法是时分和_____。
其中，局域网的介质访问控制采用的是_____技术。

解答：当多个通信设备共享某个信道时，最常用的两种复用方法是时分和_____频分_____。
其中，局域网的介质访问控制采用的是___时分___技术。

7. 选择题

假定一条线路每1/16秒采样一次，每个可能的信号变化都运载3比特的信息。问传输速率是每秒多少个比特？

a. 16bps
b. 3bps
c. 24bps
d. 48bps

解答：d

8. 填空

调制解调器（Modem）的解调器是将____信号转换成___信号；
编码解码器（Codec）的编码器是将_____信号转换成___信号。
解答：调制解调器（Modem）的解调器是将__模拟__信号转换成__数字_信号；
编码解码器（Codec）的编码器是将___模拟__信号转换成__数字_信号。

9. 选择题

信道容量是带宽与信噪比的函数，以下哪一个术语用来描述这种关系？（ ）

A. Shannon 定理　　B. 带宽　　C. Nyquist 准则　　D. 傅里叶原理

解答：A. Shannon 定理

10. 填空

一个无噪声的4000Hz的信道，若只用两种电平状态来表示信号，则信道所能达到的最大数据速率为____比特/秒。但是，若用四种不同的电平状态来表示信号，则信道上的最高码元速率为____波特。

解答：一个无噪声的4000Hz的信道，若只用两种电平状态来表示信号，则信道所能达到的最大数据速率为__8000__比特/秒($2H\log_2 V$)。但是，若用四种不同的电平状态来表示信号，则信道上的最高码元速率（采样速率）为 __8000__波特(每秒采样2H次)。

11. 选择题

半双工支持哪一种类型的数据流？

a. 一个方向
b. 同时在两个方向上
c. 两个方向，但每一时刻仅可以在一个方向上有数据流

解答：c

12. 选择题

在下列传输介质中，哪一种错误率最低？

a. 同轴电缆

b. 光缆
c. 微波
d. 双绞线

解答：b

13. 选择题

多路复用器的主要功能是什么？

a. 执行数/模转换
b. 减少主机的通信处理负荷
c. 结合来自两条或更多条线路的传输
d. 执行串行/并行转换

解答：c

14. 多路复用的主要目的是什么？

解答：使用多路复用技术的主要目的是通过在同一物理通路上发送多路信号来达到减少成本的效果。

15. 信令的定义是什么？

解答：计算机跟网络媒体交互并沿着媒体发送信号的过程称作信令。

16. 试描述统计式TDM的技术概念。

解答：统计式多路复用为要发送的每个设备分配时间，并且每个设备必须按照规定的次序发送。然而，如果一个设备没有数据要发送，那么复用器会跳过该设备，并转向下一个设备。对于共享同一传输媒体的多个系统，统计式复用是一个非常经济有效的方法。大多数计算机网络都使用某种形式的统计复用，因为在网络上的设备不需要在所有的时间都发送数据，并且是以不同的速率产生数据。

17. 为什么数字信号的衰减要比模拟信号的衰减快？

解答：当数字信号沿着“线路”传播得越来越远时，波形变化的明快程度不如初始那样显然。当波形开始变得圆滑时，接收方在信号边缘是圆滑而不是方形的情况下难以鉴别高值和低值。数字信号的这一特征使得它的衰减要比模拟信号的衰减快。

18. 将下列描述跟调制技术相匹配。一个设备类型可以用一次，多次，或根本不用。而对于每一个描述仅有一个正确的设备类型。

设备类型　a. DCE
　　b. DTE
　　c. 硬件接口

描述

_____1. 实际地处理和使用数据

_____2. 例子包括调制解调器或数字服务装置
_____3. 处理信号使其跟线路规范相一致
_____4. 在处理机和调制解调器之间传送信息
_____5. 例子包括终端和主计算机

解答： 1. b
2. a
3. a
4. c
5. b

19. 把下列的描述跟复用类型相匹配。每种复用类型可以使用一次、多次或根本不用。对应每一个描述仅可以有一个正确的复用类型。

复用类型： a. 频分
b. 时分
c. 统计复用

描述：

_____1. 免除了对调制解调器的需求，因为它使用模拟技术
_____2. 智能多路复用，能够最大限度地使用线路
_____3. 把通道划分成若干个较慢的窄的子信道
_____4. 把固定的时槽分配给每条传输线路，不管它的用户是否有数据要
传输

解答： 1. a
2. c
3. a
4. b

20．填空

根据RS-232-C标准，在传送每一字符或每一比特块之前，DTE都要把_____电路置成ON状态，DCE作为响应动作把_____电路也置成ON状态。而在每一字符或比特块传送结束时，这两个电路都会被关闭。如果在这里发生的握手过程是基于字符的，可以推断，与RS-232-C相邻的高层采用_____步协议。如果在这里发生的握手过程是基于比特块的，可以推断，与RS-232-C相邻的高层采用_____步协议。

解答：根据RS-232-C 标准，在传送每一字符或每一比特块之前，DTE都要把 RTS 电路置成ON状态，DCE作为响应动作把 CTS 电路也置成ON状态。而在每一字符或比特块传送结束时，这两个电路都会被关闭。如果在这里发生的握手过程是基于字符的，可以推断，与RS-232-C相邻的高层采用 异 步协议。如果在这里发生的握手过程是基于比特块的，可以推断，与RS-232-C相邻的高层采用 同 步协议。

21．将下列描述跟交换技术相匹配。一种交换技术可以用一次，多次，或根本不用。而对于每一个描述仅有一种正确的交换技术。

交换技术　a. 电路交换
　　b. 报文交换
　　c. 分组交换

描述

_____1. 必须在传输数据之前建立铜线通路
_____2. 适用于交互式数据处理的高速交换形式
_____3. 被进行话音通信的电话系统所采用的交换形式
_____4. 在每个中间交换站都要把用户报文存储在磁盘上
_____5. 在时间的任一点上都限制可以传输的数据量

解答： 1. a
2. c
3. a
4. b
5. c

22. 选择题

TDM的设计利用了传输媒体的什么性质？

a. 媒体的带宽大于结合信号的位速率。
b. 媒体的带宽小于单个信号的带宽。
c. 媒体的位速率小于最小信号的带宽。
d. 媒体的位速率大于单个信号的位速率。

解答：d.

23．填空

RS-232-C是一个典型的物理层协议，根据RS-232-C标准的规定：

（1）为了表示逻辑1或MARK条件，驱动器必须使用在_____伏和_____伏之间的一个电压。

（2）为了表示逻辑0或SPACE条件，驱动器必须使用在_____伏和_____伏之间的一个电压。

（3）作为DTE和DCE之间的接口，RS-232-C使用_____接插件，其中插座用于_____方，插头用于_____方。

（4）只有当_____处于ON状态时，DCE才能将DSR置成ON 状态。

（5）CTS是对RTS的_____条件，同时DSR是_____条件情况下的响应。

解答：

（1）-5伏和-15伏

（2）+5伏和+15伏
（3）DB-25, DCE, DTE
（4）DTR
（5）ON, ON

24. 就FDM而言，什么是CCITT主群标准？

解答：主群是CCITT标准中5个超群的集合。FDM主要用于AM无线电广播和话音级电话通道。在世界范围内的FDM方案已经在一定程度上得到了标准化，把12个4000Hz的话音通道复用到60kHz至108kHz的频带。在指定频率范围上这个话音通道的集合称作群。12个话音通道中的每一个都包括用户使用的3000Hz，再加上为每个话音通道保留的两个500Hz警戒带。这些警戒带帮助减少来自诸如电火花之类的干扰，因为过滤器不会产生带有陡的边缘的波。在某些环境中也有使用12kHz至60kHz频带的另一个群的情况。把5个群（或60个话音通道）复用到一起就形成一个超群。在CCITT标准中，主群是5个超群的集合。

25. 选择题
什么是WDM?

a. 在光缆上多路复用。
b. 使用传输媒体的密度进行复用。
c. 一种监视WAN延迟的流控形式。
d. 对WAN做拥塞管理的一种形式。

解答：a.

26. PCM代表什么？它通常用在什么地方？

解答：PCM代表Pulse Code Modulation（脉冲编码调制）。它通常用在电话系统，对模拟数据进行采样。

27. 使用多个接收缓冲区使得硬件接口可以有更多的时间把信息传送给CPU。试举出具有这种额外时间的两个优点。

解答：（1）防止数据溢出
（2）允许硬件接口执行简单的错误检查

28. 相当于一个T3的CCITT标准是什么？

解答：4个复用的T’2。CCITT对于每一级都定义4个载波的复用，也就是说，一个T’3的CCITT标准是4个T’2的结合。在贝尔系统中，T2和T3的位速率分别是6.312Mbps和44.736Mbps，结合4个T1（每个位速率都是1.544Mbps）产生一个T2，结合6个T2产生一个 T3。对应于T1、T2和T3的CCITT标准分别是2.048Mbps(T’1)、8.848Mbps(T’2)和34.304Mbps(T’3)，即相当于结合4个T’1产生一个T’2，结合4个T’2产生一个T’3。

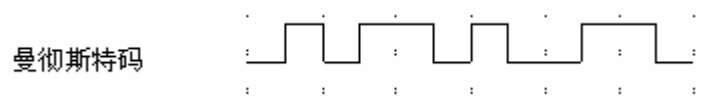
29. 试给出编码的定义。

解答：编码的作用是定义表示数据的信号的性质。

30. 在频分复用的传输链路上各个具体的信号是如何保持分离的？

解答：使用不同的载波频率运载不同的信号，这样它们就可以使用同一传输媒体而又不会互相干扰。

31. 从下图中所示的曼彻斯特编码波形所得到的二进制代码是什么？



解答：0 0 1 1 0 1。

32. 数据通信中，频带传输时可采用（A）技术的调制解调器；基带传输的编码方式可采用（B）；脉冲编码调制可采用（C）技术；多路复用时可采用（D）方法。

可供选择的答案：

A、B、C、D：1.差分PCM；2. 相移键控法PSK；3差分曼彻斯特编码；4. CRC；5. FDM；

答题填空：A(　　)；B(　　)；C(　　)；D(　　)。

解答：

A(2. 相移键控法PSK)；　　B(3差分曼彻斯特编码)；

C(1.差分PCM)；　　D(5. FDM)。

33. 已知基带数字信号为10001011，试画出差分曼彻斯特编码信号图。

解答：见图2-1

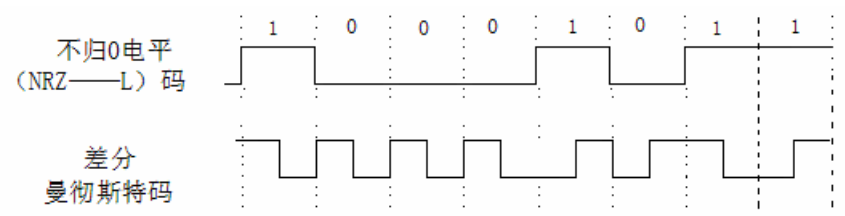


图 2-1　习题 33 插图

34. 比特率和波特率之间的差别是什么？

解答：波特率是在给定的导线上每秒钟发送的脉冲的个数。而比特率则是在给定的导线上每秒钟发送的数据位（1或0）的个数。

2.3　综合应用练习题

1. 某调制解调器使用坐标图中（1，1）、（2，2）、（-2，-2）和（-1，-1）表示4个

数据点。这个调制解调器是使用_____调制技术，它在1200波特的线路上可以达到的数据传输速率是_____。

解答：相幅联合调制，2400bps。

2．无线电天线通常在其直径等于无线电波的波长的情况下工作效果最好。合理的天线直径的范围是从1厘米到5米。问所覆盖的频率范围是怎样的？

解答：$\lambda f = c$, $c=3x10^8$ (m/s)

对于λ=1厘米，我们得到

$$f = \frac{c}{\lambda} = \frac{3x10^8}{0.01} = 3x10^{10}$$，即30GHZ

对于λ=5米，我们得到

$$f = \frac{c}{\lambda} = \frac{3x10^8}{0.01} = 0.6x10^8 = 60x10^6$$，即30GHZ

因此，所覆盖的频率范围是从60MHz到30GHz。

3．在铱计划中的66颗低轨卫星被划分成围绕地球的6个项链。在它们所使用的高度上，周期是90分钟。那么对于一个静止的发送站转交的平均间隔时间有多长？

解答：每个项链有66÷6=11颗卫星，每90分钟有11颗卫星通过头顶。这就意味着每过491秒有一次转变。这是因为60秒×90÷11≈491秒，而491秒合8分11秒，所以大约每过8分钟11秒有1次转交。

4. 一个无噪音4kHz信道每毫秒采样一次。问最大数据速率是多少？

解答：不管采样速率如何，一个无噪音信道都可以运载任意大数量的信息，因为每个采样都可以发送大量数据。事实上，对于4kHz信道，以高于每秒8kHz的速率采样是没有意义的。现在每秒采样1000次（每毫秒采样一次），如果每次采样是16位，数据速率可达16kbps，如果每次采样是1024位，则数据速率是1.024Mbps。当然，对于通常的4kHz通道，由于受仙农限制的约束，不可能达到这么高的速率。

5. 电视频道的带宽是6MHz，如果使用4级数字信号，每秒能发送多少比特？假定为无噪声信道。

解答：使用奈魁斯特定理，我们可以每秒采样12M次。4级信号意味着每次采样提供2比特，因此总的数据速率是24Mbps。

6. 一个用于发送二进制信号的3kHz信道，其信噪比为20分贝，可以取得的最大数据速率是多少？

解答：$20=10^{\log_{10}100}$

仙农极限是$3^{\log_2}(1+100)= 3^{\log_2}101=3\times6.66=19.98$kbps

奈魁斯特极限是6kbps
显然，瓶颈是奈魁斯特极限，最大数据速率是6kbps。

7. 在50kHz线路上使用T1载波需要多大的信噪比？

解答：为发送T1信号，我们需要

$$H\log_2(1+\frac{S}{N})$$

$$=1.544 \times 10^6$$

$$H = 50000$$

$$\frac{S}{N} = 2^{31} - 1$$

$10^{\log_{10}}（2^{31}-1）\approx 93$ （分贝）

因此，在50kHz线路上使用T1载波需要93分贝的信噪比。

8．在光纤网络中，无源星和有源中继器有什么区别？

解答：无源星没有电子器件，来自一条光纤的光照亮若干其它光纤。有源中继器把光信号转换成电信号以作进一步的处理。

9. 奈魁斯特定理适用于光纤吗？还是仅适用于铜线？

解答：奈魁斯特定理是一个数学性质，不涉及技术处理。该定理说，如果你有一个函数，它的傅里叶频谱不包含高于f的正弦或余弦，那么以2f的频率采样该函数，那么你就可以获取该函数所包含的全部信息。因此奈魁斯特定理适用于所有介质。

10．如果波长等于1μm，那么在0.1μm的频道中可以有多大的带宽？

解答：

$$f=\frac{c}{\lambda} \qquad \frac{df}{d\lambda}=\frac{c}{\lambda^2} \qquad df=\frac{c}{\lambda^2}d\lambda$$

$$\Delta f=\frac{c}{\lambda^2}\Delta\lambda \quad c=3x10^8\,m \quad \lambda=10^{-6}\,m$$

$$\Delta\lambda=0.1\times10^{-6}=10^{-7}\,m$$

$$\Delta f=\frac{3\times10^8}{(10^{-6})^2}\times10^{-7}=3000x10^9\,Hz$$

$$=3000GHz$$

因此，在0.1μm的频段中可以有30000GHz的带宽。

11．现在要在光纤上发送一个计算机屏幕图像序列。屏幕大小为480x640象素，每个象素24位，每秒60幅屏幕图像。问需要多大的带宽？假定每赫兹调制一个比特，那么对于中心波长为1.30μm的波段，这个带宽所对应的波长范围有多大？

解答：数据速率是480x640x24x60 bps，即442Mbps

$$\Delta f=4.42\ x\ 10^8$$

$$f=\frac{c}{\lambda} \qquad \frac{df}{d\lambda}=-\frac{c}{\lambda^2}$$

$$|\Delta\lambda|=\frac{\lambda^2\Delta f}{c}=\frac{(1.3x10^{-6})^2\,x4.42x10^8}{3x10^8}$$

$=2.5x10^{-12}\,m$ ， 即2.5x10^{-6}微米

因此，需要442 Mbps的带宽， 对应的波长范围是2.5 x 10^{-6}微米。

12. 当两束波180^{o}异相时，多路衰减的效应最明显。对于50公里长的1GHz微波链路，要使衰减最大，则路径的差别需要多大？

解答：1GHz微波的波长是30厘米（=30x10000x1000x100÷10^9）。如果一个波比另一个波多行进15厘米，那么它们到达时将180^{o}异相。显然，答案跟链路长度是50公里的事实无关。

13. 光通过玻璃的衰减取决于光的波长。图2-2给出了每公里直线距离用玻璃制作的光纤对光衰减的分贝数，其计算公式如下：

衰减的分贝数 $=10^{\log_{10}}$（传输的能量 / 接收的能量）

通信使用的波段有三个，它们分别位于0.85μm、1.30μm和1.55μm 三个中心点附近。三个波段的频率范围大约相等，都是25000GHz∽30000GHz。从图中可以看出，最左边的波段的波长范围比其它两个窄。这是为什么？

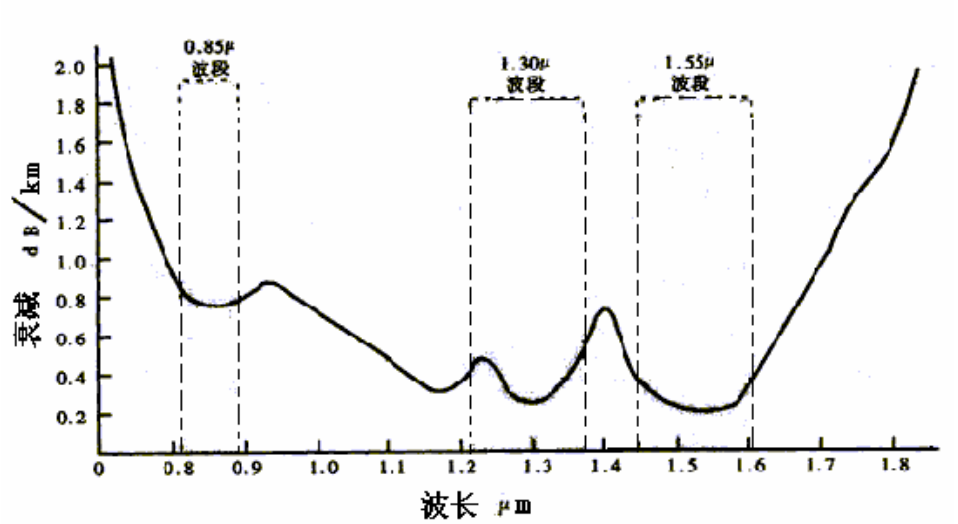


图 2-2　习题 13 插图

解答：题目已经说明，三个波段的频率范围大约相等，且从左向右三个波段的中心波长分别是0.85μm、1.30μm和1.55μm。根据公式

$$\Delta f = \frac{c}{\lambda^2}\Delta\lambda$$

显然，λ小的波段（最左边的波段λ最小）△λ也小，才能保持Δf大约相等。事实上△λ和λ是二次方的关系。顺便指出，3个带宽大致相同的事实是所使用的种类的硅的一个碰巧的特性的反映。

14. 一束1毫米宽的激光对准了100米远处的屋顶上的1毫米宽的检测器。若要使激光器偏离开检测器，光束需偏转多大的角度？

解答：如果光束在终点偏离1毫米，那么它将错开检测器。如图2-3所示，这相当于一个三角形，底长100米，高0.001米。

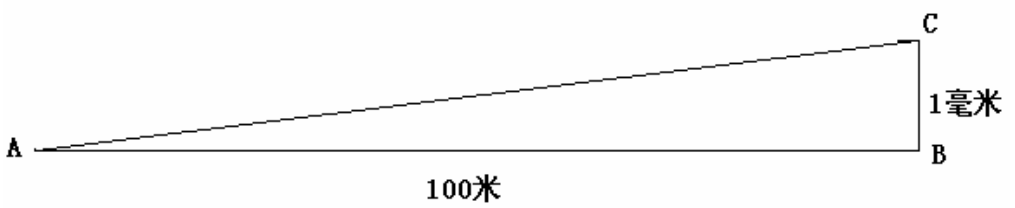


图 2-3　习题 14 插图

当A很小时，tgA≈A（弧度）

tgA=0.00001

$$A \approx 0.00001x\frac{360^0}{2\pi} \approx 0.00057^0$$

因此光束需偏转0.00057度。

15. 一个简单的电话系统由两个端局和一个长途局连接而成，端局和长途局间由1MHz的全双工主干连接。在8小时工作日中，平均一部电话使用4次，每次的平均使用时间为6分钟。10%的通话是长途的（即通过长途局）。一个端局能支持的最大电话数是多少（假定每条线路4kHz）？

解答：每部电话每小时做0.5次通话，每次通话6分钟。因此一部电话每小时占用一条电路3分钟，60分÷3分=20，即20部电话可共享一条线路。由于只有10%的呼叫是长途，所以200部电话占用一条完全时间的长途线路。局间干线复用了1000000÷4000=250条线路，每条线路支持200部电话，因此，一个端局可以支持的电话部数为200x250=50000。

16. 假定一个区域电话公司有1000万个用户，每部电话都通过铜双绞线连接到中心局，这些双绞线的平均长度是10公里。问本地回路的铜价值多少？假定每束线的直径为1毫米，铜的比重为9.0，铜的价格是每公斤3美元。

解答：双绞线的每一条导线的截面积是 π （1÷2）^{2} =0.25 π 平方毫米，每根双绞线的两条导线在10公里长的情况下体积是$0.25\pi \times (10^{-3})^2 \times 10 \times 1000 \times 2 = 0.5\pi \times 10^{-2}$ 立方米，即约为15708立方厘米。由于铜的比重等于9.0克/厘米^3，每个本地回路的质量为$9 \times 15708 = 141372$克，约为141公斤。这样，电话公司拥有的本地回路的总质量等于 $141 \times 1000 \times 10^4 \approx 1.4 \times 10^9$公斤。由于每公斤铜的价格是3美元，所以总的价值等于

$3 \times 1.4 \times 10^9 = 4.2 \times 10^9$美元。

17.考虑一颗卫星处在对地同步卫星的高度，但其轨道平面相对赤道平面倾斜角度 ϕ。对于在地球表面北纬 ϕ 度的静止用户，这颗卫星看起来在空中是动还是不动？如果回答是动的，请描述其移动。

解答：卫星从正上方（头顶）向着往南的水平线移动,离开垂直的最大偏移角度是2 ϕ。从正上方到最大偏移、再回到正上方共花24小时的时间。

18. 在1984年以前，美国电话系统的每个端局用它的3个数字的区域码和本地号码的开头3个数字命名。区域码用2-9范围内的一个数字开头，第2个数字可以是0或1，末尾的第3个数字可以是任何数字。本地号码的开头两个数字总是在范围2-9内，第3个数字可以是任何数字。那么，在1984年以前可以有多少个端局？

解答：区域码的个数有8×2×10=160。本地号码的3位前缀的个数有8×8×10=640。

160×640=102，400

因此端局的个数被限制到102，400。显然，这个限制不是一个问题。

19. 在美国，电话号码采用10个数字表示，大约有22，000个端局，每个端局最多有10，000条电话线路。如果不改变编号方案，也不增加设备，那么实际可以支持的电话数目有多少？假定每条电话线路仅有一个设备。

解答：使用10个数字的电话号码，总共可以有10^{10}个号码，虽然其中有许多区域号码

（例如000）是非法的。然而更主要的限制来自端局的个数。有22，000个端局，每个端局最多有10，000条线路。这就意味着电话的最大数目是220×10^6，即2亿2千万部。实际上可以连接的数目还到不了这么多，因为一些端局是不满的。在一个小城镇中的端局附近可能没有10，000个客户，因此有好多线路只能被浪费掉。

20. 高性能微处理器价格的降低使得有可能在每个调制解调器中都装上一个，这样对电话线路的出错处理有什么样的影响？

解答：通常在物理层对于在线路上发送的比特不采取任何差错纠正措施。在每个调制解调器中都包括一个CPU使得有可能在第一层中包含错误纠正码，从而大大减少第二层所看到的错误率。由调制解调器做的错误处理可以对第二层完全透明。现在许多调制解调器都有内建的错误处理功能。

21. 一个输油管道是一个单工系统、半双工系统、全双工系统，还是三者都不是？

解答：像是一个单轨火车道，它是半双工。油在两个方向上都可以流动，但不能同时在两个方向上流动。

22. 在一个星座图中（用于Modem）,所有的点都位于一个以原点为中心的园上。这里使用的是哪一种调制？

解答：如果所有的点都和原点等距离，它们都具有相同的振幅，因此不是使用振幅调制。频率调制永远不会用于星座图。因此该编码是纯粹的相移键控。

23. 一个调制解调器的星座图与图2-4（相位幅度联合调制）相似，它在如下坐标处有数据点：（1，1），（1，-1），（-1，1）和（-1，-1）。则这个调制解调器在1200波特的线路上可以达到多大的数据传输速率？

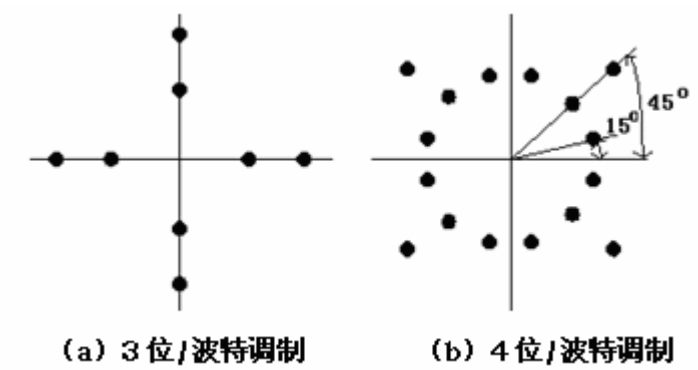


图 2-4　习题 23 插图

解答：每个波特有4个合法值，因此比特率是波特率的两倍。对应于1200波特，数据速率是2400bps。

24. 一个调制解调器的星座图与上题中的插图相似，它在（0，1）和（0，2）处有数据点。这个调制解调器使用的是相位调制还是幅度调制？

解答：相位总是0，但使用两个振幅，因此这是直接的幅度调制。

25. 一个全双工QAM-64 Modem使用多少个频率？

解答：两个。一个用于上行，另一个用于下行。调制机制本身仅使用振幅和相位，频率没有被调制。

26. 一个使用DMT (Discrete Multi—Tone modulation: 离散多音频调制)的ADSL系统把3/4的可用数据通道分配给下行链路。它在每个通道上都使用QAM-64调制。那么，下行链路的容量是多少？

解答：总共有256个通道，除去6个用于POTS的通道，再除去用于控制的2个通道，剩下248个通道用于数据。如果这些通道中的3/4用于下行链路，那么有186个通道用于下行。ADSL调制是在4000波特上进行的，因此使用QAM-64（每波特6位），186个通道中的每一个都有24，000bps的数据速率。因此总的下行带宽是4.464Mbps。

27. 在如图2-5（LMDS系统体系结构）所示的4区段LMDS（Local Multipoint Distribution: 本地多点分布业务）示例中，每个区段都有它自己的36Mbps通道。按照排队理论，如果该通道50%加载，那么排队时间将等于下载时间。在这些条件下，下载5kB的Web页面要花多长的时间？在1Mbps的ADSL线路上下载该页面要花多长时间？在56kbps的Modem上呢？

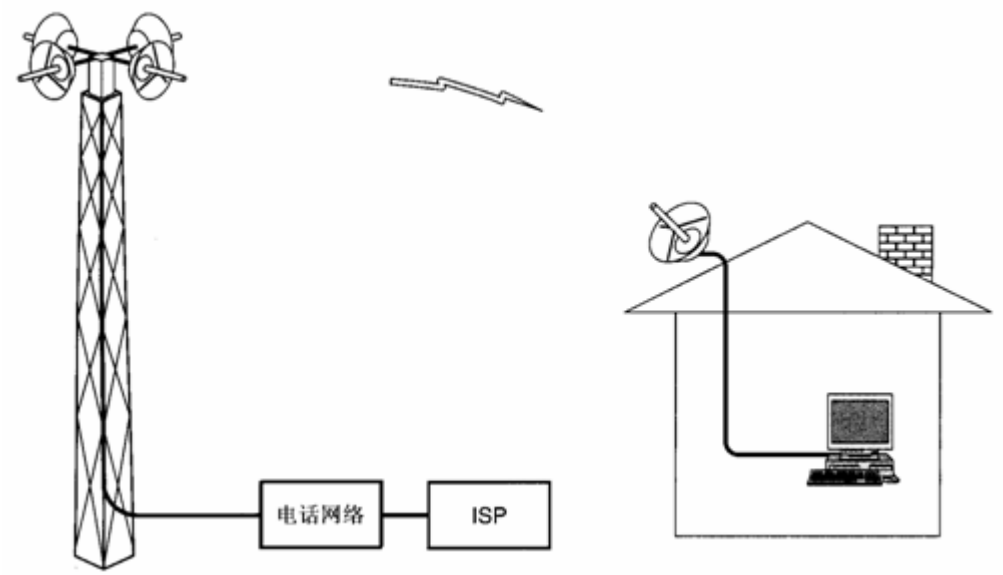


图 2-5　习题 27 插图

解答：5kB的Web页面有40，000位。在36Mbps通道上的下载时间是1.1毫秒。如果排队延迟也是1.1毫秒，总时间是2.2毫秒。

在ADSL上没有排队延迟，因此在1Mbps速率下的下载时间是40毫秒。
在56kbps的Modem上的下载时间是714毫秒。

28. 有10个信号，每个需要4，000Hz。它们使用FDM被复用到单个通道。该复用通道

所需要的最小带宽是多少？假定警戒带是400Hz宽。

解答：有10个4，000Hz信号，我们需要9个警戒带以避免干扰。这样所需要的最小带宽等于4，000×10+400×9=43，600Hz。

29. FTTH（光纤到住家）适合于电话公司的端局、长途局等的模型吗？或者该模型必须作根本改变？请解释你的答案。

解答：完全适合。在光纤和双绞线之间的接线盒只是一个新的种类的交换局，因此，等级结构就变成：区域局，地区局，主局，长途局，端局和接线盒。

30. 在低端，电话系统是星型的，所有邻近的本地回路都汇集到一个端局。与之相反的是有线电视，由一条很长的电缆把所有邻近的房屋都串接在一起。假定将来的电视线缆是10Gbps的光纤而不是铜线，那么它可以用来模拟电话模型，让每个人都有自己到达端局的线路吗？如果可以，多少个有一部电话的家庭可以连到同一路光纤上？

解答：可以，每部电话都能够有自己到达端局的线路，但每路光纤都可以连接许多部电话。忽略语音压缩，一部数字PCM电话需要64kbps的带宽。如果我们以64kbps为单元来分割10Gbps，我们得到每路光缆串行156250家。现今的有线电视系统每根电缆串行数百家。

31. 一个有线电视系统有100个商用频道，所有的频道都交替地播放电视节目和广告。它是像TDM还是像FDM？

解答：它既像TDM，也像FDM。100个频道中的每一个都分配有自己的频带（FDM），在每个频道上又都有两个逻辑流通过TDM交织播放（节目和广告交替使用频道）。

32. 为什么把PCM采样时间设置成125微妙？

解答：125每秒的采样时间对应于每秒8000次采样。一个典型的电话通道是4kHz。根据奈魁斯特定理，为获取在一个4kHz通道中的全部信息需要每秒8000次的采样频率。

33. T1线路的开销比例有多大？即1.544Mbps中有多少比例没有投递给端点用户？

解答：T1载波处理复用在一起的24条话音信道。24条信道轮流将其采样的8位数字插入输出串，其中7位是用户数据，1位是控制信号。1帧包含24x8=192比特和一个附加的帧位（用于帧同步），这样每125微妙193比特，总的数据率是1.544Mbps。由于在一个帧中，端点用户使用193位中的168（=7x24）位，开销占25（=193-168）位，因此开销比例等于

25÷193≈13%.

34. 比较在下列两种情况下一个无噪音4kHz信道的最大数据速率：

（1）使用每次采样产生2比特的模拟信号编码

（2）使用T1 PCM系统

解答：在两种情况下都可以每秒采样8000次。在每秒采样产生2比特的模拟信号编码的情况下，每次采样发送2位，最大数据速率可达2x8000=16000bps，即16kbps。对于T1，每个采样周期发送7位数据，最大数据速率为7x8000=56000bps，即56kbps。

35. 如果一个T1传输系统一旦失去了同步，它就会尝试使用每一帧中的第一位重新同步。问平均要查看多少帧才能重新取得同步且保证误判率不超过0.001？

解答：10个帧。在数字通道上某些随机比特是0101010101模式的概率是

$$\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times\frac{1}{2}\times=\frac{1}{1024}$$

察看10个帧，若每一帧中的第一位形成比特串0101010101，则判断同步成功，但误判的概率为1/1024，小于0.001。

36. 调制解调器的解调部分和编码解码器的编码部分都能把模拟信号转换成数字信号。它们之间有区别吗？若有，是什么？

解答：有。编码器接受任意的模拟信号，并从它产生数字信号。而解调器仅仅接受调制了的正弦（或余弦）波，产生数字信号。

37. 一个信号在4kHz的无噪声信道上以数字方式传送，每125微妙采样一次。在采用如下编码方法时，每秒钟实际发送的比特数是多少？

（a）CCITT 2.048 Mbps标准

（b）有4位相对信号值的DPCM

（c）增量调制

解答：

（a）CCITT 2.048Mbps标准用32个8位数据样本组成一个125微妙的基本帧，30个信道用于传信息，2个信道用于传控制信号。在每一个4kHz信道上发送的数据率就是8x8000=64kbps。

（b）差分脉码调制（DPCM）是一种压缩传输信息量的方法，它发送的不是每一次抽样的二进制编码值，而是两次抽样的差值的二进制编码。现在相对差值是4位，所以对应每个4kHz信道实际发送的比特速率为4x8000=32kbps。

（c）增量调制的基本思想是：当抽样时间间隔t_s很短时，模拟数据在两次抽样之间的变化很小，可以选择一个合适的量化值△作为阶距。把两次抽样的差别近似为不是增加一个△就是减少一个△。这样只需用1比特二进制信息就可以表示一次抽样结果，而不会引入很大误差。因此，此时对应每个4kHz信道实际发送的数据速率为1x8000=8kbps。

38. 为了提供比STS-1低的数据速率，SONET有一个虚拟支流（VT）系统。一个虚拟支流是可以插进STS-1帧的部分载荷，它可以跟其他的部分载荷相结合以填充数据帧。VT1.5使用STS-1帧的3列，VT2使用4列，VT3使用6列，VT6使用12列。试问：哪个VT可以提供

（a）一个DS-1业务（1.544Mbps）？

（b）欧洲的CEPT业务（2.048Mbps）？

（c）一个DS-2业务(6.312Mbps)？

解答：VT1.5可以提供

8位×3(列) ×9(行) ×8,000(帧/秒) = 1.728Mbps，

可以用它来提供DS-1业务。

VT2可以提供

8位×4(列) ×9(行) ×8,000(帧/秒) = 2.304Mbps，

可以用它来提供CEPT-1业务。

VT6可以提供

8位×12(列) ×9(行) ×8,000(帧/秒) = 6.912Mbps，

可以用它来提供DS-2业务。

39. 对于幅度为A的纯粹正弦波按增量调制编码，每秒x次采样。输出+1对应信号变化+A/8，输出-1对应信号变化-A/8。在无积累误差的前提下，可以跟踪的最大频率是多少？

解答：在波的四分之一周期内信号必须从0上升到A。为了能够跟踪信号，在T/4的时间内（假定波的周期是T）必须采样8次，即每一个全波采样32次，采样的时间间隔是1/x，因此波的全周期必须足够地长，使得能包含32次采样，即T≧32/x，或f≦x/32.

因此，可以跟踪的最大频率是x/32.

40. SONET时钟的漂移率大约为10^{-9}，则需化多长时间才能使漂移相当于1比特宽？该计算结果有什么含义？

解答：10^{-9}的漂移率意味着10^{9}秒中的1秒，或每秒中的一个毫微妙。对于OC-1速率，即51.840Mbps，取近似值50Mbps，大约一位持续20毫微妙。这就说明每隔20秒钟，时钟就要偏离1位。这就说明，时钟必须连续进行同步，才能保持不会偏离太大。

41．OC-3的用户数据传输速率是148.608Mbps。请问如何从SONET 的OC-3参数推导出该值？

解答：基本的SONET帧是每125微妙产生810字节。由于SONET是同步的，因此不论是否有数据，帧都被发送出去。每秒8000帧与数字电话系统中使用的PCM信道的采样频率完全一样。

810字节的SONET帧通常用90列乘以9行的矩形来描述，每秒传送8x810x8000=51840000bps，即51.84Mbps。这就是基本的SONET信道，它被称作同步传输信号STS-1，所有的SONET干线都是由多条STS-1构成的。

每一帧的前3列被留作系统管理信息使用，前3行包含段开销，后6行包含线路开销。剩下的87列包含87x9x8x8000=50112000bps，即50.112Mbps的数据。被称作同步载荷信封的数据可以在帧的任何位置开始。线路开销的第一行包含指向第一字节的指针。同步载荷信封（SPE）的第一列是通路开销。

通路开销不是严格的SONET结构，它嵌入在载荷信封中。通路开销端到端地流过网络，因此把它跟端到端地运载用户信息的SPE相关联是有意义的。然而，它确实从可提供给端点用户的50.112Mbps中又减去1x9x8x8000=576000bps，即0.576Mbps，使之变成49.536Mbps。

OC-3相当于3个OC-1复用在一起，因此其用户数据传输速率是49.536x3=148.608Mbps。

42. 在一条OC-12c连接中可提供的用户带宽是多少？

解答：当一条线路（例如OC-3）没有被多路复用，而仅从一个源输入数据时，字母c（表示concatenation, 即串联）被加到名字标识的后面。因此，OC-3表示由3条单独的OC-1线路复用成155.52Mbps线路，而OC-3c表示来自单个源的155.52Mbps的数据流。OC-3c流中所包含的3个OC-1流按列交织编排，首先是流1的第1列，流2的第1列，流3的第1列，随后是流1的第2列，流2的第2列，……，依此类推，最后形成270列宽9行高的帧。

OC-3c流中的用户实际数据传输速率比OC-3流的速率略高（149.760Mbps和148.608Mbps），因为通路开销仅在SPE中出现1次，而不是当使用3条单独OC-1流时出现的3次。换句话说，OC-3c中270列中的260列可用于用户数据，而在OC-3中仅能使用258列。更高层次的串联帧（如OC-12c）也存在。

OC-12c帧有12x90=1080列和9行。其中段开销和线路开销占12x3=36列，这样同步载荷信封就有1080-36=1044列。SPE中仅1列用于通路开销，结果就是1043列用于用户数据。由于每列9个字节，因此一个OC-12c帧中用户数据比特数是8x9x1043=75096。每秒8000帧，得到用户数据速率

75096x8000=600768000bps，即600.768Mbps。

所以，在一条OC-12c 连接中可提供的用户带宽是600.768Mbps。

43. 一个电缆公司决定在一个有5，000家的社区中提供Internet访问。该公司使用一条同轴电缆和一种频谱分配方案，允许每条电缆有100Mbps的下行带宽。为了吸引客户，公司决定在任何时间都保证每家至少有2Mbps的下行带宽。该电缆公司需要怎样做才能提供这一保证。

解答：对每家2Mbps的下行带宽保证意味着每条同轴电缆最多穿行50家。因此，电缆公司将需要把现有的电缆分裂成100条同轴电缆，并且把它们中的每一条都直接连接到一个光纤节点。

44. 使用如图2-6（在典型的有线电视系统中用于Internet访问的频率分配）所示的频谱分配方案，一个电缆系统把多少Mbps分配给上行带宽？把多少Mbps分配给下行带宽？

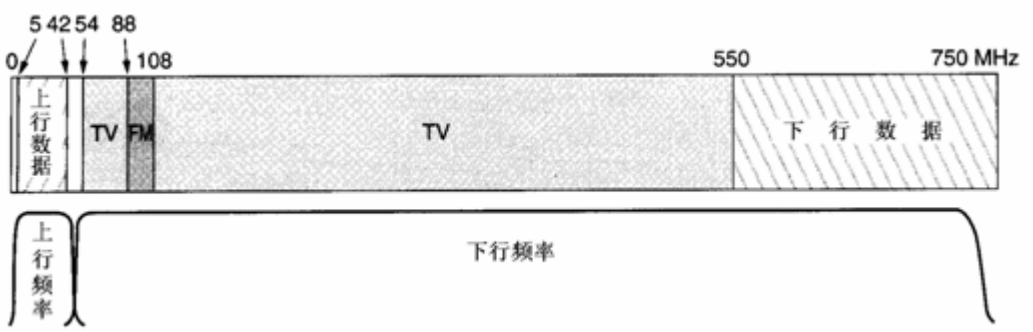


图 2-6 习题 44 插图

解答：上行带宽是37Mbps。使用QPSK,每赫兹调制2位，得到74Mbps的上行带宽。下行带宽有200MHz;使用QAM-64，可得到1200Mbps的下行带宽；使用QAM-256，可得到1600Mbps的下行带宽。

45. 在没有其它网络交通的情况下，一个电缆用户接收数据的速率可以有多大？

解答：通常的方案是对每个6MHz下行通道使用QAM-64调制，所取得的数据速率大约36Mbps，去掉开销，净荷大约27Mbps。即使下行通道以27 Mbps工作。用户接口总是10Mbps的以太网。在这样的条件下，不可能使计算机的输入速率大于10Mbps。如果在PC和电缆Modem之间的连接是快速以太网，那么可提供完全的27Mbps。通常电缆运营商指定10Mbps以太网，因为他们不想让一个用户消耗掉整个带宽。

46．有时候，当一个蜂窝用户穿越边界从一个单元进入另一单元时，当前的呼叫会突然中止，尽管所有的发射设备和接收设备都工作正常。这是为什么？

解答：频率不能够在邻接的单元中重用，因此，当一个用户从一个单元移动到另一单元时，必须为该呼叫分配一个新的频率。如果一个用户移动到一个其所有频率都正在被使用的单元，那么该用户的呼叫必须被终止。

47. 如果一个卫星正处在地球上空20000英里位置，那么一个信号需用多少时间才能从地面送至卫星并从卫星返回？（假定信号以光速传播，卫星转发需时53微秒）

解答：1英里=1.61公里　20000英里=32200公里

32200公里/（300000公里/秒）=322/3000秒

（322/3000）x 2 x 1000 + 53/1000≈214.72毫秒

因此，一个信号需用214.72毫秒的时间才能从地面送至卫星并从卫星返回。

48．为了在面积等于120平方公里的某城市建立个人通信服务（PCS），大约要划分成多少个直径为100米的微单元才能覆盖全市？

解答：如果我们假定每个微单元是直径为100米的园，那么每个微单元的面积是π(100÷2)^2=2500π（平方米），以次去划分120平方公里的平面，可达到

$120\times10^6 \div 2500\pi \approx 15279$ 个微单元。

当然，用园形来铺砌平面是不可能全覆盖的。下面考虑使用六边形（参见图2-7，一个划分成六边形单元的典型的蜂窝电话系统）。

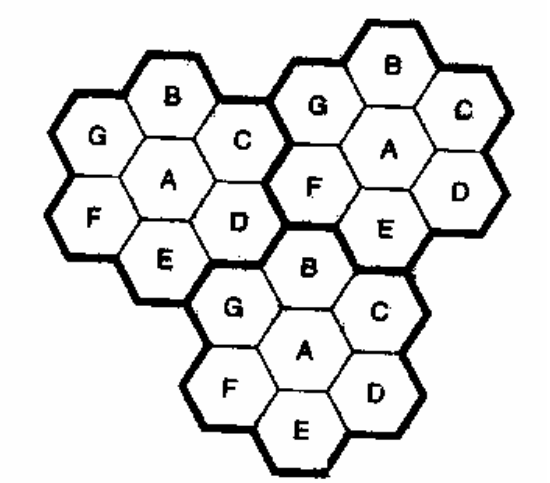


图 2-7 习题 48 插图

每个六边形的面积可以用6个边长等于50（=100/2）米的等边三角形的面积和表示。每个三角形的面积等于

$$\frac{1}{2}\times 50\times\frac{1}{2}\sqrt{3}\times 50=\frac{1}{2}\times 50\times\frac{1}{2}\times 1.7321\times 50=1082.56$$ （平方米）

六边形的面积等于

$$1082.56\times 6\approx 6495.36$$ （平方米）

$$\frac{120\times 10^{6}}{6495.36}\approx 18475$$ （个微单元）

考虑到城市面积的实际形状和实际实施全覆盖所采用的微单元平面形状的灵活性，大约用20000个微单元可以实际地覆盖全市。

49．在两个通信的DTE之间的一个传输通道由三个部分组成。第一部分引入16dB的衰减，第二部分引入20dB的增益，第三部分引入10dB的衰减。假定平均发射功率是400Mw，试计算该通道的平均输出功率。

解答：对于第一部分，

$$16=10\log_{10}\frac{400}{P_2}$$

因此P_2= 10.0475mW。

对于第二部分，

$$20=10\log_{10}\frac{P_2}{10.0475}$$

因此P_2 = 1004.75mW。

对于第三部分，

$$10 = 10 \log_{10} \frac{1004.75}{P_2}$$

因此$P_2 = 100.475mW$。

即平均输出功率100.475mW。

或者

因此$P_2 = 1004.75mW$。

对于第三部分，

$$10 = 10 \log_{10} \frac{1004.75}{P_2}$$

因此$P_2 = 100.475mW$。

即平均输出功率100.475mW。

或者

由通道的总衰减 （16—2 0）+ 10 = 6 dB

得到

$$6 = 10 \log_{10} \frac{400}{P_2}$$

所以$P_2 = 100.475mW$。

50．使用每个信号元素8个电平级的传输方案在PSTN上传输数据。如果PSTN的带宽是3000Hz，试求出Nyquist最大数据传输速率C和调制效率B。

解答：$C = 2W\log_2 M$

现在W = 3000Hz， M = 8

所以 $C = 2 \times 3000 \times \log_2 8 = 2 \times 3000 \times 3 = 18000bps$

B = R/W

现在 R = 18000bps，W = 3000Hz

所以B = 18000÷3000 = 6 bps/Hz

51．假定PSTN的带宽是3000Hz，典型的信噪功率比是20dB，试确定可以取得的理论上最大的信息（数据）速率。

解答：

$$SNR = 10 \log_{10} \frac{S}{N}$$

因此， $$20 = 10 \log_{10} \frac{S}{N}$$

$$\frac{S}{N} = 100$$

现在，

$$C = W \log_2 (1 + \frac{S}{N})$$

因此，$C = 3000 \times \log_2(1+100) = 19\ 936$ bps

即可以取得的理论上最大的信息（数据）速率是19 936 bps。

52．在带宽为3000Hz的PSTN上传输数据。如果在接收端平均信噪功率比是12dB，试确定可以取得的最大数据速率R。假定

（a）$E_b/N_0 = 13$dB

（b）$E_b/N_0 = 10$dB

这里的E_b是在信号中以每比特焦耳（=瓦特×秒）为单位计量的能量，N_0是以每赫兹瓦特为单位计量的噪音功率密度。

试同时计算在这两种情况下的带宽效率B。

解答：

$$10\log_{10} R = \frac{S}{N} + 10\log_{10} W - \frac{E_b}{N_0}$$

带宽效率B = R/W

（a）$10\log_{10}R = 12+10\log_{10}3000-13=33.77$

因此，R = 2382.32 bps，B = 0.79

（b）$10\log_{10}R = 12+34.77-10 = 36.77$

因此，R = 4753.35 bps，B = 1.58

53．在两个DTE之间传送1000比特的数据块。试对下列类型的链路分别计算传播延迟对发射延迟的比率。

（1）100米的双绞线和10k bps的发射速率。

（2）10k 米的同轴电缆和1M bps的发射速率。

（3）50 000k 米的自由空间（卫星链路）和10M bps的发射速率。

假定在每种类型的电缆内电信号的传播速率是2×10^8米/秒，在自由空间内信号的传播速率是3×10^8米/秒。

解答：（1）

$$T_p = \frac{S}{V} = \frac{100}{2\times10^8} = 5 \times 10^{-7} \text{秒}$$

$$T_x = \frac{N}{R} = \frac{1000}{10 \times 10^3} = 0.1 \text{秒}$$

$$a = \frac{T_p}{T_x} = \frac{5 \times 10^{-7}}{0.1} = 5 \times 10^{-6}$$

（2）

$$T_p = \frac{S}{V} = \frac{10 \times 10^3}{2 \times 10^8} = 5 \times 10^{-5} \text{秒}$$

$$T_x = \frac{N}{R} = \frac{1000}{1 \times 10^6} = 1 \times 10^{-3} \text{秒}$$

$$a = \frac{T_p}{T_x} = \frac{5 \times 10^{-5}}{1 \times 10^{-3}} = 5 \times 10^{-2}$$

（3）

$$T_p = \frac{S}{V} = \frac{5 \times 10^7}{3 \times 10^8} = 1.67 \times 10^{-1} \text{秒}$$

$$T_x = \frac{N}{R} = \frac{1000}{10 \times 10^6} = 1 \times 10^{-4} \text{秒}$$

$$a = \frac{T_p}{T_x} = \frac{1.67 \times 10^{-1}}{1 \times 10^{-4}} = 1.67 \times 10^3$$

54．在一个通信通道上发送速率为500bps的二进制信号。试计算所需要的最小带宽。假定要接收最坏情况序列，且仅传输

（a）基本频率；
（b）基本频率和三次谐波；
（c）基本频率、三次谐波和五次谐波。

解答： 就数据传输而言，所发送的二进制信息可能是任意变化的序列。考虑周期序列10101010…， 110110110110…，1110111011101110…，等等。第一个序列重复两比特为一个单元的周期，第二个序列重复三比特为一个单元的周期，…。显然，序列10101010…具有最短的周期，产生最高的基本频率成分。这就意味着，其它序列所产生的基本频率都比它低。因此，我们把这个具有最短周期的序列称为最坏序列。

在本题中，速率为500bps的最坏序列101010…具有250Hz的基本频率成分。由此可以得出，三次谐波是750Hz，五次谐波是1250Hz。在每种情况下所需要的带宽分别是：

（a）0-250　　（b）0-750Hz　　（c）0-1250Hz

55．假定使用ASK调制技术，试分别估算在比特率为300bps、1200bps和4800bps时传输数据所需要的通道带宽。

（a）要接收序列101010…的基本频率成分；
（b）要接收序列101010…的基本频率成分加上三次谐波。

请对你所得到的结果跟PSTN的关系加以评论。

解答：由于载波是单频率音频，假定是单位幅度信号，那么我们可以用下列表达式表示：

$$v_c(t) = \cos \omega_c t$$

我们还可以把具有单位幅度和基本频率 ω_0 的序列表示成：

$$v_d(t) = \frac{1}{2} + \frac{2}{\pi}\{\cos \omega_0 t - \frac{1}{3}\cos 3\omega_0 t + \frac{1}{5}\cos 5\omega_0 t - \cdots\}$$

那么 $v_{ASK}(t) = v_c(t) \cdot v_d(t)$

$$v_{ASK}(t) = \frac{1}{2}\cos \omega_c t + \frac{2}{\pi}\{\cos \omega_c t \cdot \cos \omega_0 t - \frac{1}{3}\cos \omega_c t \cdot \cos 3\omega_0 t + \cdots\}$$

$$v_{ASK}(t) = \frac{1}{2}\cos \omega_c t + \frac{1}{\pi}\{\cos(\omega_c - \omega_0)t + \cos(\omega_c + \omega_0)t - \frac{1}{3}\cos(\omega_c - 3\omega_0)t - \frac{1}{3}\cos(\omega_c + 3\omega_0)t + \cdots\}$$

所以ASK信号在频率方面可以近似为载波信号频率w_c，加上（w_c-w_0）和 (w_c+w_0)两个频率，再加上两个谐波（w_c-3w_0）和 (w_c+3w_0)。它们等距离地分布在载波的两边，并且被称作边带。

我们知道，带宽越高，所接收的信号越接近所发送的信号。然而，如果通道的带宽足以通过序列101010…的基本频率成分，就可以得到满意的操作，该序列具有基本的频率成分f_0（以Hz为单位），它等于比特率（以bps为单位）的一半。因此ASK所需要的最小带宽等于比特率（$2f_0$），但以Hz为单位。在确定所需要的最小带宽时，后面列出的两个主要带宽都是必需的。另外，如果要接收三次谐波成分，需要三倍位速率的带宽（6 f_0，以Hz为单位）。

在本题中在指定条件下的带宽需求可列表如下：

位速率	300bps	1200bps	4800bps
基本频率成分	150Hz	600Hz	2400Hz
三次谐波成分	450Hz	1800Hz	7200Hz
仅基本频率所需带宽	300Hz	1200Hz	4800Hz
基本频率加上三次谐波所需带宽	900Hz	3600Hz	14400Hz

PSTN可用的带宽是3000Hz。因此在三种位速率中，仅300bps可以接收到3次谐波。1200bps的位速率仅可以接收到基本频率成分。4800bps的位速率不能仅使用ASK传输。

56. 假定在地球和一个新月亮之间建立一条100M位/秒的链路。从该月亮到地球的距离大约是385000公里，数据在链路上以光速3×10^8米/秒传输。

（a）计算该链路的最小RTT。

解：最小RTT等于2×385000000米÷（3×10^8米/秒）=2.57秒

（b）使用RTT作为延迟，计算该链路的“延迟×带宽”值。

解：“延迟×带宽”值等于2.57秒×100M位/秒=257M位≈32M字节

（x）在（b）中计算的“延迟×带宽”值的含义是什么？

解：它表示发送方在收到一个响应之前能够发送的数据量。

（d）在月亮上用一个照相机拍取地球的相片，并把它们以数字形式保存到磁盘上。假定在地球上的任务控制要下载25M字节的最新图像，那么，从发出数据请求到传送结束最少要花多少时间？

解：在图像可以开始到达地面之前，至少需要一个RTT。假定仅有带宽延迟，那么发送需要的时间等于25M字节÷100M位/秒=200M位÷100M位/秒=2秒。所以，直到最后一个图像位到达地球，总共花的时间等于2.0+2.57=4.57秒。

57. 如图5-8所示，主机A和B每个都通过10M位/秒链路连接到交换机S。

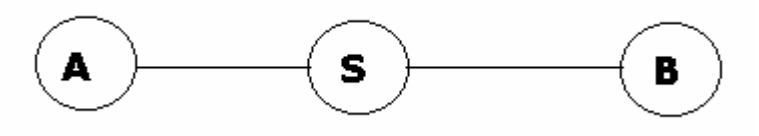


图 5-8　习题 57 插图

在每条链路上的传播延迟都是20微秒。S是一个存储转发设备，在它接收完一个分组后35微妙开始转发收到的分组。试计算把10000比特从A发送到B所需要的总时间。

（a）作为单个分组

解：每条链路的发送延迟是10000÷10M位/秒=1000微秒

总的传送时间等于$2\times1000+2\times20+35=2075$微秒。

（b）作为两个5000位的分组一个紧接着另一个发送

解：当作为两个分组发送时，下面列出的是各种事件发生的时间表：

T=0　　开始
T=500　A完成分组1的发送，开始发送分组2
T=520　分组1完全到达S
T=555　分组1从S起程前往B
T=1000　A结束了分组2的发送

T=1055 分组2从S起程前往B
T=1075 分组2的第1位开始到达B
T=1575 分组2的最后1位到达B

事实上，从开始发送到A把第2个分组的最后1位发送完经过的时间为2×500微妙，
第1个链路延迟20微妙，
交换机延迟为35微妙（然后才能开始转发第2个分组），
500微妙的发送延迟，
第2个链路延迟20微妙，
所以，总的时间等于2×500微妙+20微妙+35微妙+500微妙+20微妙=1575微妙。

第 3 章　数据链路层

本章学习重点

- 异步传输和同步传输
- 差错检测和纠正
- 自动重复请求
- 数据成帧方法
- 流控和窗口机制
- 面向比特的链路控制规程HDLC
- 面向字节的协议PPP

3.1　基本知识点

网络上两个相邻结点之间的通信，特别是通信双方的同步，是由规则和约定来支配的，这种规则和约定称为数据链路控制。数据链路控制协议的目的是为了在一给定的通信链路上提供发送端和接收端之间的无差错信息传输。

所谓“相邻”是指两个机器实际上通过一条信道直接相连，在概念上可以想象成一根导线。要使信道具有导线一样的属性，则必须使数据按比特顺序交付到目的地时与发出时顺序完全一样。实际的信道偶尔会出错，而且它们的数据传输率是有限的，同一数据位在收与发之间还存在着传输时延。这些限制，加上有限的计算机处理速度，对数据传输都有很大的影响。数据链路协议层的设计必须考虑所有这些因素，并提供适当的解决途径。

数据链路层的功能建立在一条或多条物理连接之上。它不提供分割和重组功能，来自于网络层实体的每个服务数据单元（SDU）以一对一的方式映射进数据链路协议数据单元（DL-PDU）。通常，人们把DL-PDU称作帧。

数据链路层必须负责帧的定界，实现一种能够识别帧的开始和结束的结构。帧的结构可以包含错误检测的机制，错误纠正可以通过帧的重传获得，也可以通过前向纠错编码得以实现。对于数据链路连接，还应该能够提供保序和流控功能，保证在链路层连接上收到的帧能够以和发送时同样的顺序递交给网络层实体，并协调发送方和接收方的节奏，保证发送方不会以太快的速度使得接收方被淹没。

3.1.1　异步传输和同步传输

比特的传送和接收是通过采用定时时钟来完成的。发送计算机利用它的时钟来决定每个比特的起始和结束。在接收计算机那里，时钟被用来确定对信号进行采样取值的位置和

间隔时间。一般情况下，使两个独立的时钟精确同步是不太可能的，它们都产生自己的漂移，引起两个连续采样之间的间隔比所希望的变长了或变短了。

时钟漂移会引起接收方在确定一个比特的起始和结束位置时发生错误。由于接收时钟与发送时钟的差异，接收方可能对代表1位的信号采样两次，从而多产生一个比特，也可能跳过一位。

解决上述同步问题的方法有两种。第一种称为异步法，发送方和接收方独立地产生时钟，但定期地进行同步。第二种方法称为同步法，接收端时钟完全由发送方时钟控制，也就是说，接收方时钟与发送方时钟是严格同步的。

异步传输是基于这样的事实：在一定的比特数目内，时钟漂移的程度是有限的。它让接收方在某一个时间点上跟一个发送方时钟信号同步，并由此开始自己独立的时钟信号序列。由于偏移Σ相对于一个比特时间来说是比较小的，接收方可以在偏移积累到采样发生错误之前正确地接收若干个比特。

在异步传输中，数据以字符为单元发送；每个字符的长度根据所使用的编码方案可以是5到8个比特。作为例子，常用的ASCII编码每个字符7个比特；另一种在所有的IBM机器（个人计算机除外）上采用的EBCDIC（扩展的二进制编码的十进制交换码）编码是每个字符8个比特。值得注意的是，定时或同步仅仅在每个字符的范围内维持着，接收方在每个新字符的开头都被提供机会重新进行同步。

在同步传输中，以一种稳定的流方式传送比特块，不使用开启和停止位编码。该数据块在长度上可以是许多个比特。为了防止在发送机和接收机之间的定时漂移，它们的时钟必须通过某种途径保持同步。一种可能性是在发送设备和接收设备之间提供单独的时钟线路。由一方（发送方或接收方）负责在线路上定期地加载脉冲，即每个比特周期发送一个短脉冲。另一方使用这些规则脉冲作为时钟。这种技术在短距离上工作得很好，但对于较长的距离，时钟脉冲会跟数据信号一样面临失真的问题，从而产生定时错误。另一种替代的方法是在数据信号中嵌入时钟信息；对于数字信号，这可以通过使用曼彻斯特或差分曼彻斯特编码得以实现。对于模拟信号，有多种技术可以使用；例如，可以使用载波频率本身基于载波的相位来使接收设备同步。

对于同步传输，还需要进行另一个层次上的同步，使得接收设备能够确定一个数据块的开始和结束。为了取得这一目标，每个块以一个前缀比特串开始，并且一般地还用一个后缀比特串结尾。此外，还附加一些其它的比特传递在数据链路控制过程中要使用的控制信息。数据加上前缀、后缀和控制信息就形成了帧。准确的帧格式取决于所使用的数据链路控制过程。

3.1.2　差错检测和纠正

数据通信中，利用编码方法进行差错控制的方法基本上有两类：自动请求重发（ARQ——Automatic Request for Repeat）和前向纠错（FEC——Forward Error Correction）。在ARQ方式中，接收端发现差错时，以某种方式通知发送端重发，直到收到正确的码字为止。在FEC方式中，接收端不但能发现差错，而且能确定二进制码元发生错误的位置，从而得以纠正。我们把能够自动发现差错的编码称为检错码。把不仅能发现差错而且能自动纠错的

编码称作纠错码。

差错检验编码都是采用冗余编码技术，具体方法很多，但核心思想是有效数据（信息位）在被发送前，先按照某种关系附加上一定的冗余位，构成一个符合某一规则的码字后再发送。其中要发送的有效数据变化时，相应的冗余位也随之变化，使得码字遵从不变的规则。在接收端收到码字后，判断它是否仍然符合原规则，若不符合原规则，就可以判定传输过程有错。两种常用的检错编码是奇偶检验码和循环冗余检验码。

ARQ方式只使用检错码，但必须有双向信道，才有可能把差错信息反馈到发送端；同时发送方要分配一定的数据缓冲区，把已经发送出去的数据的拷贝再存放一段时间，以便在得到发生传输差错的通知时可以重新发送。

FEC方式则必须使用纠错码，它不需要利用反向信道来传递请求重发的信息，也不需要分配实施重发的数据缓冲区。虽然FEC有上述的优点，但由于纠错码一般都要使用比检错码更多的冗余位，编码效率低，而且纠错算法也要比检错算法复杂得多，因而除非在单向传输或实时性要求特别高（FEC由于不需要重传，实时性较好）等场合外，数据通信中使用更多的还是ARQ差错控制方式。

海明码能够纠正单比特错。有一个技巧可用来使海明码能纠正突发性非单比特错。将k个码字组织成一个矩阵，每行1个码字。一般情况下，每次发1个码字，码字按位从左到右发送。为了纠正非单比特错，数据应该从最左边的1列开始发送，每次发1列，发完1列的k比特后，再发下1列，依次下去。当帧到达接收方时，每列k位重新组成矩阵，如果有k比特连续错发生，k个码字中的每一个最多只有一位受影响，而海明码能够纠正码字中的单比特错。因此，整个块都可以被恢复。这种方法使用kr个检测位，使km个数据的块能恢复长度最多为k的突发性非单比特错。

3.1.3 自动重复请求

在计算机网络的分布式环境中，有关传输媒体或通信对方机器上进程的状态不可以直接获取，就需要在源和目的站之间限制未确认应答的PDU的数量。这样才能避免源发方以传输系统不能及时投递的发送速率淹没接收设备。流量控制就是保证发送实体不会因过量的数据而把接收实体冲跨的技术。

作为例子，停止—等待式自动重复请求（ARQ）就是最基本的流控技术。源实体发送一个数据单元被接收后，由目的实体发回一个对刚收到的该数据单元的确认，用以表示它愿意接受另一个数据单元。源实体必须等待直到接收到对该数据单元的确认后才能发送下一个数据单元。因此，目的站能简单地用停发确认的方法来停止数据流动。

采用差错检测和ARQ的结果是把一条不可靠的数据链路转变成可靠的数据链路。有多种形式的ARQ，除了前述停止—等待式ARQ外，还有回退N式ARQ和选择性拒绝ARQ。

在停止——等待式ARQ中，源站发送单个PDU后必须等待确认，在目的站的回答到达源站之前，源站不能发送其它的数据PDU。在一个PDU发送之后，如果在计时器计满时仍未收到确认，则再次发送相同的PDU。重复的PDU使得接收方可能收到同一数据单元的两个副本，但却把它们当成是互相独立的，以为后来接收到的是一个新的PDU。为了避免这样的问题，发送的PDU交替地用0和1来标示，肯定确认则用ACK0和ACK1来表示。

在回退N式ARQ中，接收方应以正确的顺序把收到的报文递交给本地主机。发送方在不等确认就连续发送许多个PDU的情况下，有可能发送了N个PDU后，才发现尚未收到对前面的PDU的确认信息，也许某个PDU在传输的过程中出错了。接收方因这一PDU有错，查出后不会交给本地主机，对后面再发送来的N个PDU也可能均不接受而丢弃。换句话说，接收方只允许按顺序接收。当发送方发现前面的PDU未收到确认信息而计时器已经超时后，不得不又重发该PDU以及随后的N个PDU。正因为如此，这种ARQ称作回退N式ARQ。

为了提高信道的有效利用率，就要允许发送方不等确认PDU返回就再连续发送若干个PDU。由于允许连续发出多个未被确认的PDU，其编号就不能仅采用1个比特（只有0和1两个号码），而要采用多位PDU编号才能区分。凡是被发送出去尚未被确认的PDU都可能出错或丢失而要求重发，因而都要保留副本。这就要求发送方有较大的发送缓冲区保留准备重发的帧。

显然，允许发送未被确认的PDU越多，可能要退回来重发的PDU也越多。另外，为了控制发送方的发送速率以及受发送缓冲区大小的制约等因素都要求对发送方已发出但尚未得到确认的PDU的数目加以限制。这个数目就称为发送窗口，落在这个窗口内的PDU的号码就是等待接收方返回的确认PDU的号码。由于帧号只有有限的位数，到一定的值之后就又循环回来了。

在回退N式ARQ中，一个站可以顺序地发送一系列PDU，其编号以某个最大值为模来计算。未处理完、未被确认的PDU的数目取决于窗口大小，接收站有对每个外来的PDU都进行确认或对若干个PDU进行累积确认的选择。

在选择性拒绝ARQ中，若某一个PDU出错后，后面送来的正确PDU虽然不能立即递交给本地主机，但接收方仍可收下来，放在一个缓冲区中，同时要求发送方重新传送出错的哪一帧，一旦收到重传的PDU后，就可与原先已收到但暂存在缓冲区中的其余的PDU一起按正确的顺序送本地主机。

显然选择性拒绝ARQ在某个PDU出错时减少了后面所有的PDU都要重传的浪费，但对接收方提出了更高的要求，要有一个足够大的缓冲区来暂存未按顺序正确收到的PDU。凡是在一定范围内到达的PDU，那怕未按顺序，也要接收下来。若把这个范围看成是接收窗口的话，接收窗口的大小是大于1的；而回退N式ARQ正是接收窗口等于1（只接收顺序中的下一个PDU）的一个特例。所以说，选择性拒绝ARQ也可以看成是一种滑动窗口协议，只不过其发送窗口和接收窗口都大于1。

3.1.4　数据成帧方法

数据链路层通常把比特流划分成离散的帧，并对每一帧计算出检验和。字符计数法、字节填充法和位填充法是3种常用的成帧方法。

字符计数法是在帧头部使用一个字段来标明帧内字符数。

字节填充法使用标志字节和字节填充，通常采用的措施是每一帧以ASCII字符序列DLE STX开头，以DLE ETX结束。DLE代表Data Link Escape; STX代表Start of Text; ETX代表End of Text。用这种方法，目的机器一旦丢失帧边界，它只须查找DLE STX或DLE ETX字符序列，就可以找到所在的位置。

当传送像是目标程序或浮点数这样的二进制数据时， DLE STX或DLE ETX可能出现在用户的数据段中，这时，发送方的数据链路层需要在数据段中的每个DLE字符前面再插入一个DLE的ASCII代码。接收方的数据链路层在将数据交给网络层之前丢掉这个DLE字符。正因为如此，该方法称作字节填充法。

位填充法允许数据帧包含任意个数的比特，也允许每个字符的编码包含任意个数的比特。开头和结尾使用标志字节01111110，当发送方的数据链路层在数据段中遇到5个连续的1时，它自动在其后插入一个0。当接收方看到5个连续的1后面跟着一个0时，自动将此0删去。正因为如此，该方法称着位填充。

3.1.5 面向比特的链路控制规程HDLC

高级数据链路控制（HDLC）是由国际标准化组织制定的面向位的有序链路级协议。在HDLC中，任何必须在两个站之间交换的控制信息都被放在传送帧的特别段中；这些段相对帧的边界有固定的位置。HDLC的主要功能目标有三个方面：

① 保证发射的数位流具有透明性；
② 确定发送帧的格式及帧内段的含义；
③ 实现链路上站之间的协调，保证有序交换。

为了满足对具有广泛的适应性的通用数据链路控制规程的要求，HDLC定义了三种不同的站类型，两种链路结构和三种数据传输方式。三种站类型是主站、次站和复合站。主站控制着数据链路（通道），它向信道上的次站发送命令帧，依次接收来自次站的响应帧。如果这条链路是多点共享的，那么主站负责跟连在该链路上的每一个站维持一个单独的会话。次站辅助主站工作；它是一个被动的角色，接收来自主站的命令并作出响应。次站只维持一个会话，那就是它和主站之间的会话。复合站既发送命令和响应，也接收来自另一个复合站的命令和响应。它维持着它跟另一个复合站之间的会话。

两种链路结构是非平衡型和平衡型。在非平衡结构中，有一个主站和一个或多个次站，以点对点或多点共享、半双工或全双工、交换型或非交换型等方式工作。这种结构之所以称为非平衡的，是因为主站负责控制每个次站，并负责建立置方式命令。在平衡结构中，两个复合站点对点地互连。信道可以是半双工或全双工，可以是交换型或非交换型。两个复合站在信道上处于同等的地位，可以互相发送未经邀请的数据帧。每个站都有同等的链路控制责任。

三种数据传输方式是通常响应方式、异步响应方式和异步平衡方式。在通常响应方式（用于非平衡型结构）中，次站必须在得到主站明确的许可之后才可以发送。在接到许可后，次站启动一次可以包含数据的响应传输。在次站的响应传输期间，通道就被次站占用；次站可以在此期间发送一个或多个帧。在发送完最后一个帧之后，次站必须再等待得到明确的许可才可以再次发送。

在异步响应方式（也用于非平衡型结构）中，每当发现链路空闲时，不论是主站还是次站，都可以发送；也就是说，允许次站未得到主站许可就启动发送。传送可以包含一个或多个数据帧，也可以包含反映次站状态变化的控制信息。这种工作方式可以降低开销，

因为次站不需要轮询序列就可以发送数据。多点配置有时以一种竞争的方式进行操作，连接在一起的工作站都可以自由地发送。两个站同时传输将会引起数据破坏。仅当同时传输的可能性很小时，竞争方式才是一种成功的操作。显然，有一小部分应用可能需要在多点配置的异步响应方式中操作，HDLC并不禁止使用这种方式。

异步平衡方式提供了在两个逻辑上地位平等的站（即两个复合站）之间的平衡型数据传输方式。一个复合站没有得到另一个复合站的许可就能启动发送。对于点对点结构，异步方式通常比正常响应方式效率更高，因为异步方式不需要轮询。

HDLC的帧格式，它是由标志、地址、控制、信息和帧检验序列（FCS）等段构成的。HDLC允许有3种类型的帧：

（1）信息帧：用于数据传输，还可以同时用来对已收到的数据进行确认和执行轮询等功能。

（2）监控帧：用于数据流控制，帧本身不包含数据，但可执行对信息帧确认、请求重发信息帧和请求暂停发送信息帧等功能。

（3）无编号帧：主要用于控制链路本身，它不使用发送或接收帧序号。某些无编号帧可以包含数据。

在HDLC中，地址可以是接收站的，也可以是发送站的，这取决于所使用的过程类别。在非平衡配置中，有一个主站和一个或多个次站。每个次站都分配一个具唯一性的地址。此外，某些地址可能被分配给不止一个站。这些地址称作组地址。使用一个组地址发送的帧将被该组中所有的站接收。全1被保留给链路上的所有站，也称广播地址。发送的命令帧里总是带有接收站的地址。发送的响应帧里总是带有发送站的地址。地址段的长度可以是1个字节或多个字节。在使用多字节地址（扩展寻址）的情况下，每个字节中最低位是1时，表示这是地址的最后一个字节；最低位是0时，说明后随的字节还表示地址。

3.1.6　面向字节的协议PPP

PPP（点到点的协议）是使用串行线路通信的面向字节的协议。它既可以在异步线路上使用，也可以在同步线路上使用；不仅用于拨号MODEM链路，也用于租用的路由器到路由器的线路。

PPP最初的出现是用作在点到点链路上传输IP交通的封装协议。PPP还建立一套标准，以便于IP地址的分配和管理，异步的（起停位的）和面向位的同步封装，网络协议的多路复用，链路配置，链路质量测试，错误检测 ，以及对于诸如网络层地址和数据压缩这样的功能的选项协商。PPP 通过提供一个可扩展的链路控制协议（LCP）和一个网络控制协议（NCP）族来协商选项配置参数和设施。除了IP之外，PPP还支持其它协议，包括Novell的互连网络分组交换（IPX）和DECnet。

PPP包含三个主要成分，即HDLC封装、链路控制协议和网络控制协议。它们分别提供下列三个方面的功能：

（1）一种成帧方法，明确地定界一个帧的结束和下一个帧的开始，其帧格式也允许进行错误检测。

（2）一个链路控制协议，负责线路建立、测试和选项协商，并在它们不再被需要时，稳妥地把它们释放。该协议被称作链路控制协议（LCP）。

（3）一种协商网络层选项的方式，对于所支持的每一个网络层协议都有一个不同的网络控制协议（NCP），用来建立和配置不同的网络层协议。PPP被设计成允许同时使用多个网络层协议。

为了在点到点的链路上建立通信，呼叫方PPP首先发送LCP帧，配置和（可选地）测试数据链路。在配置了链路并协商好LCP所需要的可选设施之后，呼叫方PPP发送NCP帧选择和配置一个或多个网络层协议。在配置完所选择的每一个网络层协议后，来自每个网络层协议的分组就都可以在链路上发送了。该链路一直处于已配置好可用于通信的状态，直到有显式的LCP帧关闭链路，或者发生了某个外部事件（例如不活动期超时或用户干预）为止。

PPP的帧格式非常类似于HDLC的帧格式，它们之间的主要不同点在于PPP是面向字节的，而不是面向位的。特别地，PPP在拨号MODEM线路上使用字符填充，因此所有的帧的长度都是整数个字节。例如，在HDLC中，你发送一个由30.25个字节组成的帧是可能的，而在PPP中就不可能。

所有的PPP帧都以标准的HDLC标志字节01111110开头，如果它出现在载荷段中就要做字符填充，使用的控制转义字节是01111101。为了实现透明传输，发送方在对帧进行FCS计算之后，要检查在头尾标志之间整个帧，把可能有的每个标志字节用控制转义字节加上标志字节所组成的二字节序列代替；把可能有的控制转义字节用由两个控制转义字节组成的二字节序列代替。在接收方则要执行相反的操作。

接在标志字节后面的是地址段，它总是被设置成二进制值11111111，表示所有的站都要接收它。使用这个数值就避免了必须分配数据链路地址的问题。

地址段的后面是控制段，其缺省值是00000011，这个值表示一个无编号帧。换句话说，作为缺省条件，PPP不提供使用序列号和确认应答的可靠传输。在有噪音的环境中，比如无线网络，可以使用编号方式的可靠传输(通过LCP确定）。

第四个PPP段是协议段，它的任务是说明在载荷段中运载的是什么种类的分组。已经为LCP、NCP、AppleTalk和其它协议定义了代码。以比特0开始的协议是诸如IP、IPX和AppleTalk这样的网络层协议，例如，0021（H）表示IP，002b（H）表示IPX，0029（H）表示AppleTalk。以比特1开始的协议被用来协商其它协议，它们包括LCP以及针对每个所支持的网络层协议的一个不同的NCP。例如，c021（H）表示LCP，8021（H）表示IP控制协议，802b（H）表示IPX控制协议，8029（H）表示AppleTalk控制协议。协议段的缺省长度是2字节，但它可以使用LCP协商变成1个字节。作为例子，图3-12示出了一个带有IP数据报的PPP帧格式。

载荷段的长度是可变的，可以协商一个最大值。如果在线路建立期间没有协商长度，就采用缺省长度1500字节。如果需要，在载荷的后面可以有填充。

在载荷段的后面是检验和段，它通常是2个字节，但也可以通过协商使用4个字节的检验和。

总之，PPP是一个适用于MODEM、HDLC位串行线路、SONET和其它物理层的多协议

成帧机制。它支持错误检测、选项协商、头部压缩和（可选的）使用HDLC成帧的可靠传输。

3.2　基本练习题

1. 选择题

下列哪种错误检查方法常被用来在面向字符的传输协议中产生块检查字符（BCC）？

a. 奇检验
b. 偶检验
c. 水平奇偶检验
d. 循环冗余检验

解答：c

2. 选择题

下列哪一项最好地描述了循环冗余检验的特征？

a. 逐个地检查每一个字符
b. 查出99%以上的差错
c. 查不出有偶数个位出错的差错
d. 不如纵向冗余检查可靠

解答：b

3．假定我们要发送信息11001001，并且使用CRC多项式x^3+1来检错

（a）使用多项式长除来确定应该发送的信息块。

解答：取信息11001001，附加000，并用1001去除，余数是011.
应该发送的信息块是11001001011.

（b）假定信息块最左边的比特由于在传输链路上的噪音而变化，接收方CRC计算的结果是什么？接收方是怎样知道发生了错误的？

解答：把第1位变反，得到01001001011，再用1001去除，得到商01000001，余数是10。由于余数不为零，所以接收方知道发生了错误。

4．在一条HDLC链路上，下列位序列到达接收节点

11010 11111010 111110010 11111 0110

试给出发送方在进行位填充之前对应这个位序列的二进制数据。

解答：11010 11111 1011111 1011111 01011111 110

5．给出一个例子，说明4位错不会被两维奇偶检查发现。试给出4位错不会被两维奇偶检查发现的一般情况说明。

解答：在数据的2维排列中，如果把一个矩形的四个角上的二进制数都变反，那么所有的奇偶位仍然正确。反过来讲，如果有4位改变了还发现不了错误，那么错误位一定形成一个矩形。因此，如果经过两维奇偶检查没有发现错误，那么要么每1行和每1列都没有错误，要么跟错误位相关的每1行和每1列都有两个错。

6. 假定一个成帧协议使用比特充填，示出当帧包含下列比特序列时在链路上发送的比特序列。

11010111110101111101011111110

解答：11010111110<u>0</u>01011111<u>0</u>10101111<u>0</u>110

7. 选择题

BSC被看成是哪种类型的数据链路协议？

a. 面向位的 DDCMP
b. 面向字节计数的
c. 面向字符的
d. 面向分组的

解答：c

8. 选择题

在下列协议中，哪一种使用带位填充的首尾标志法组帧？

a. DDCMP
b. HDLC
c. BSC
d. SLIP

解答：b

9. 试描述称为偶检验和奇检验的差错检测方法。

解答：偶检验的计算是统计在位流中1的个数，如果1的个数是奇数，就把奇偶位置成1，使得在数据和奇偶位中1的总个数是一个偶数。奇检验跟偶检验相反，在数据和奇偶位中1的总个数应该是一个偶数。

10. 选择题

前向纠错的实现是：

a. 错误检测码　　b. 按字节计算的错误编码
c. 按位计算的错误编码　　d. 差错纠正码

解答：d. 差错纠正码有时也称作前向纠错码或FEC。

11. 确认应答的目的是什么？

解答：确认应答通常是一个特别的控制帧，它所包含的信息对所收到的信息做表示正确收到的肯定应答，或做表示发生了差错的否定应答。

12. 下列字符串的16位检验和是什么？

GiGGle

解答：用十六进制来表示，字符串gi=6769，GG=4747，le=6c65，所以GiGGle的16位检验和等于6769+4747+6c65=11B15,其中最左边的1是进位，所以最终的检验和等于1B16。

13. 假定一条通信链路正在经受干扰，使得每个第18位都从0变成1，或从0变成1。奇偶位能够发现所有的错误吗？

解答：不能够。奇偶检查在有奇数个位被改变了的情况下能够有效地发现传输差错，但当有偶数个位被改变了的时候不能够正确地指示差错。

14. CRC的计算可以用软件执行，但大多数实现都使用专门为CRC做的硬件。试解释这是为什么？

解答：大多数实现都使用CRC硬件，这是因为它简单，硬件执行速度快，并且做起来便宜。

15. 下列字符块是BSC协议从相邻高层接收来的数据的一部分，准备组帧交给物理层传送。为了能够以透明方式传送，请按照字符填充算法写出填充后放在帧的数据段中的对应这个字符块的输出。

DLE　STX　C　DLE　A　DLE　ETX

解答：

DLE　DLE　STX　C　DLE　DLE　A　DLE　DLE　ETX 。

16．图3-1中通信的两个站采用HDLC协议，交换的帧用“地址+帧名+N（S）值+P/F+N（R）值”的形式表示，P和$\overline{P}$分别表示P位置成1和0，F和$\overline{F}$分别表示F位置成1和0，在帧中不使用的段用一表示。请根据给出的一个帧序列完成下列问题填充：

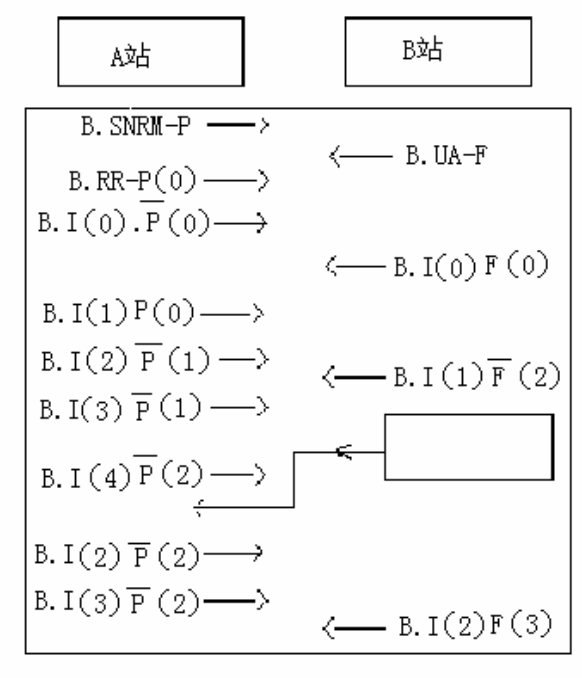


图 3-1　习题 16 插图

（1）它们使用的是HDLC的_____通信方式。

（2）所进行的是_____　通信。

（a）全双工
（b）半双工

（3）由B站发往A站的帧“B.I(2)F(3)”是 _____。

（a）命令
（b）响应

在发此帧时，B已经成功地收到了由A发往B的第____号帧 。

（4）在帧序列中用长方形表示的空白中正确的帧的格式应该是_____。

解答：

(1) 它们使用的是HDLC的 正常响应 通信方式。

(2) 所进行的是 全双工 通信。

(a) 全双工
(b) 半双工

(3) 由B站发往A站的帧“B.I(2)F(3)”是 响应 。

(a) 命令
(b) 响应

在发此帧时，B已经成功地收到了由A发往B的第 2 号帧 。

(1) 在帧序列中用长方形表示的空白中正确的帧的格式应该是 B.REJ-$\overline{F}$(2) 。

17. 下列比特块是HDLC协议从相邻高层接收来的数据的一部分，准备组帧交给物理层传送，为了能够以透明方式传送，请按照位填充算法写出填充后放在帧的数据段中的对应这个比特块的输出。

0 1 1 1 1 1 0 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1 0

解答：

0 1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 1 0 1 0 1 1 1 1 1 0 1 1 0 。

18. 为什么使用停止-等待式的协议在卫星通信链路上具有低的吞吐率？

解答：在停止-等待式协议中，发送方每发送一个分组后都要等待确认应答，然后才能发送下一个分组。卫星传输具有长的延迟，在停止-等待式协议中，每发送一个分组后发送方必须等待确认应答的时间是该延迟的两倍，这就进一步减低了在卫星链路上的吞吐率。

19. 为提供比使用单个奇偶位可能得到的更大可靠性，一种检错编码方案使用一个奇偶位检测所有的奇数位，用第二个奇偶位检测所有的偶数位。那么此代码的海明距离是多少？

解答：由于奇偶位性质，对任何有效码字做一个改变不会产生另一个有效码字。对偶数位做两个改变或对奇数位做两个改变将产生另一个有效码字，因此海明距离是2。

20. 信息有效数据m是每个字符用7比特字节编码的ASCII码串“well”，即m长28位，其中，w=1110111，e=1100101，l=1101100，取多项式CRC-12=$X^{12}+X^{11}+X^3+X^2+X+1$做循环冗余检验编码，求该码串的冗余部分r（要求写出主要的计算步骤）。

解答：用被除数=1110111 1100101 1101100 1101100 000000000000

除数=1100 0000 01111

做二进制除法，得到商=1011010 1010101 1001000 1010110

余数r=1111 0001 0010，因此该码串的冗余部分r就等于1111 0001 0010。

3.3 综合应用练习题

1．下面的表中给出了字母D、E和F的7比特ASCII码表示。采用偶检验，求出传送的信息为DEF时检验比特及块检验字符BCC

	b_6	b_5	b_4	b_3	b_2	b_1	b_0
D	1	0	0	0	1	0	0
E	1	0	0	0	1	0	1
F	1	0	0	0	1	1	0

解答：

	b_6	b_5	b_4	b_3	b_2	b_1	b_0	b_7
D	1	0	0	0	1	0	0	**0**
E	1	0	0	0	1	0	1	**1**
F	1	0	0	0	1	1	0	**1**
BCC	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**

2. 在网络传输中解决差错问题的一种方法是在每个要发送的字符或数据块上附加足够的冗余信息，使接收方能够推导出发送方实际送出的应该是什么内容。请根据能够纠正单比特错的海明编码方法对ASCII字符Z（二进制编码是1011010）形成11位码字。要求简要地写出编码过程，并说明在传输过程中有一位错的情况下如何能够检查出是哪一位错。

解答：m=7,r=4,n=11。

编号1=1，2=2，3=1+2，4=4，5=1+4，6=2+4，7=1+2+4，8=8，9=1+8，10=2+8，11=1+2+8，于是有：

(1) ——>(1)+(3)+(5)+(7)+(9)+(11)

(2) ——>(2)+(3)+(6)+(7)+(10)+(11)

(4) ——>(4)+(5)+(6)+(7)

(8) ——>(8)+(9)+(10)+(11)

编号：	1	2	3	4	5	6	7	8	9	10	11
码字：	0	0	1	*0*	0	1	1	1	0	1	0

当一码字到达时，接收方将计数器清零。然后接收方检查每个校验位D，看是否具有

正确的奇偶性，这里的D是检验位的编号。如果第D位奇偶性不对，则计数值加D。若所有校验位被检查过后，计数器值仍为0，这个码字就作为有效码字接受。假如计数器值不为0，则该值就是出错位的编号。

3．在使用位填充的情况下，对于丢失、插入或修改单个位的错误，检验和是否可能发现不了？如果不可能，为什么不？如果可能，怎么回事？在这里检验和的长度起作用吗？

解答：可能。假定原来的正文包含位序列01111110作为数据。位填充之后，这个序列将变成011111010。如果由于传输错误第二个0丢失了，收到的位串又变成01111110，被接收方看成是帧尾。然后接收方在该串的前面寻找检验和，并对它进行验证。如果检验和是16位，那么被错误地看成是检验和的16位的内容碰巧经验证后仍然正确的概率是$1/2^{16}$。如果这种概率的条件成立了，就会导致不正确的帧被接受。显然，检验和段越长，传输错误不被发现的概率会越低，但该概率永远不等于零。

4．在一个数据链路协议中使用下列字符编码：

A: 01000111;　　B: 11100011;　　FLAG: 01111110;　　ESC: 11100000

在使用下列成帧方法的情况下，说明为传送4个字符A、B、ESC、 FLAG所组织的帧实际发送的二进制位序列：

（a） 字符计数

解答：00000100　01000111111000111111000000001111110

（b）使用标志字节和字节填充

解答：01111110　01000111　11100011　11100000　11100000　11100000　01111110　01111110

（以标志字节开头和结尾；如果数据中有FLAG，则在其前面加ESC；如果数据中有ESC，则将其双写。）

（c）开头和结尾使用标志字节，并使用位填充

解答：01111110　0100011111100011111100000　011111010　01111110

5．下列数据片断发生在一个数据流的中间，如果使用字节填充算法，那么填充之后对应该片段的输出是什么？

A　B　　ESC　C. ESC　　FLAG　　FLAG　　D

解答：A　B　ESC　ESC　C　　ESC ESC　　ESC FLAG　ESC　FLAG　　D

6．有人说，每一帧用一个FLAG字节结尾，再用一个FLAG字节表示下一帧的开头，这样做是浪费的。用一个FLAG字节可以同时表示前一个帧的结束和下一个帧的开始。他们认为节省一个字节总是好的。你同意这种说法吗？如果有不同意见，请说明原因。

解答：如果有一个无休止的帧流，一个标志字节可能是足够的。然而，如果一个帧结束了（带有一个FLAG字节），并且在15分钟内没有新帧，那么接收方怎么知道下一个字节实际上是一个新帧的开始，还是仅仅是线路上的噪音呢？使用开始的FLAG标志和结束的

FLAG标志，协议就会简单得多。

7．图3-2中通信的两个站都是采用HDLC 协议的复合站，交换的帧用“地址+帧名+N（S）值+P/S+N（R）值”的形式表示，$\overline{P}$ 表示P位置零，在帧中不使用的段用—表示。

请根据所给出的帧序列回答问题。

（1）它们使用的是HDLC 的哪一种通信方式？

（2）序列中使用的I帧和RR 帧是命令还是响应？

信息帧使用的编号规则的模数是几？用于应答机制的窗口有多大？

从发往A 的帧“A.I(6).P(7)”中可以推断，在发此帧时，B已经成功地收到了由A发往B的第几号帧？

序列中属于无编号帧类型的有哪几个？

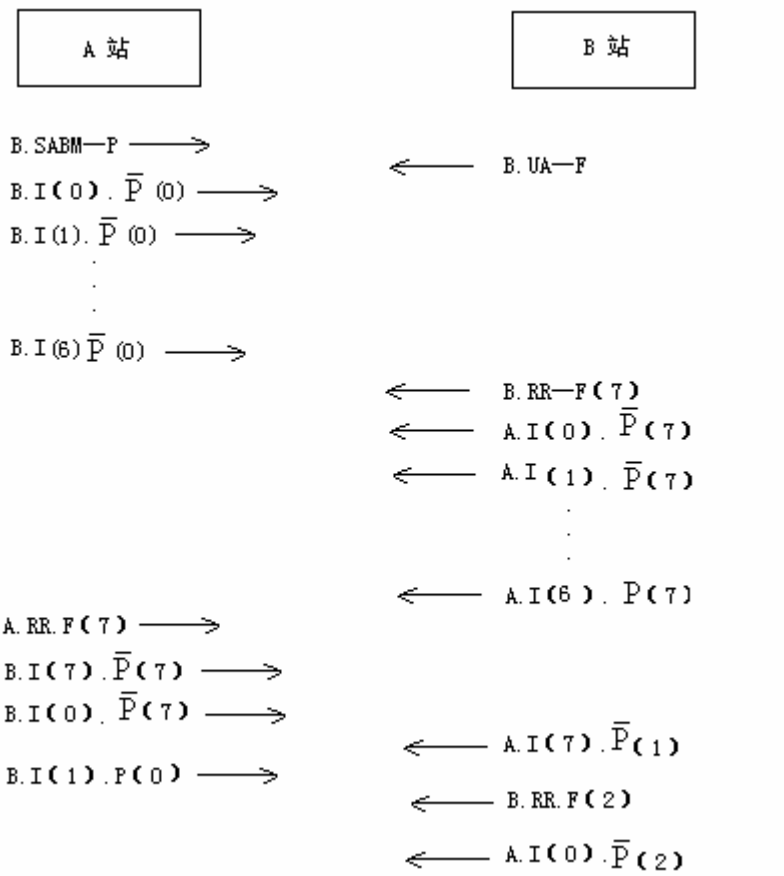


图 3-2　习题 7 插图

解答：

（1）它们使用的是HDLC 的异步平衡方式。

（2）序列中使用的I帧是命令，RR 帧是响应。

（3）信息帧使用的编号规则的模数是8，用于应答机制的窗口尺寸为7。

（4）从发往A 的帧“A.I(6).P(7)”中可以推断，在发此帧时，B已经成功地收到了由A发往B的第6号帧。

（5）序列中属于无编号帧类型的有：置异步平衡方式（SABM）和无编号确认（UA）。

8．使用海明编码发送16位报文。需要多少个检查位可以保证接收方能够监测并纠正单个位错？说明对于报文1101001100110101发送的位图案。假定在海明编码中使用偶检验。

解答：在海明编码中，假定有m个信息位和r个检查位，并且允许单个错可以被纠正。对应2^m个合法消息中的每一个都有n个跟它相距1的非法码字。它们是通过把n位码字中的每一位变反形成的。这样2^m个合法消息中的每一个都有n+1种位图案相对应。由于n=m+r,位图案总数是2^n，显然必须使（n+1）$2^m \leqslant 2^n$，将n=m+r代入，得到

（m+r+1）$\leqslant$ 2^r,

这一关系式可以由海明提出的组码方法得以保证。将最终码字各位从1开始依次由左向右编号，让是2的幂的序号的位成为检查位，其余位填充m位数据。每个检查位都是包括它自己在内的某个位集合计算偶（或奇）检验的结果。一个数据位跟哪n个检查位有关可以通过将其序号写成2的幂的和的形式得知。例如，11=1+2+8，29=1+4+8+16，那么（11，1，2，8）和（29，1，4，8，16）都是检查奇偶性的位集合。

在本题中m=16, 在最后码字的1、2、4、8和16位置上加检查位，r=5。由于包括检查位在内，码字长度不会超过31，所以5个奇偶位足够了。

0　1　1 1 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 1

1=1，　2=2，　3=1+2，　4=4，　5=1+4，　6=2+4，　7=1+2+4，　8=8，9=1+8，10=2+8，11=1+2+8，12=4+8，13=1+4+8，14=2+4+8，15=1+2+4+8，16=16，17=1+16，18=2+16，19=1+2+16，20=4+16，21=1+4+16

所以，1 –〉1+3+5+7+9+11+13+15+17+19+21

2 –〉2+3+6+7+10+11+14+15+18+19

4 –〉4+5+6+7+12+13+14+15+20+21

8 –〉8+9+10+11+12+13+14+15

16 –〉16+17+18+19+20+21

所以发送的位图案是 01111011001100111010 1.

9．一个8位字节10101111使用偶检验海明编码, 编码后的二进制值是什么?

解答：m=8,在1、2、4和8位上加检查位，码字长度不会超过15，所以4个奇偶位足够了。

1=1，　2=2，　3=1+2，4=4，5=1+4，6=2+4，7=1+2+4，8=8，9=1+8，10=2+8，11=1+2+8，12=4+8，

所以，1 -〉1+3+5+7+9+11

2 -〉2+3+6+7+10+11

4 -〉4+5+6+7+12

8 -〉8+9+10+11+12

1 0 1 0 0 1 0 0 1 1 1 1

1-> 1+0+0+1+1=1 (3+5+7+9+11)

2-> 1+1+0+1+1=0 (3+6+7+10+11)

4-> 0+1+0+1=0　(5+6+7+12)

8->0+1+1+1+1=0 (9+10+11+12)

所以，编码的二进制值是 101001001111。

10．一个12位的海明码到达接收方时的十六进制值是0×E4F,那么，原先的值用十六进制表示是什么样子？假定传输差错不超过1位。

解答： 1 1 1 0 0 1 0 0 1 1 1 1

1-〉3+5+7+9+11 –〉1+0+0+1+1 –〉1

2-〉3+6+7+10+11-〉1+1+0+1+1-〉0

4-〉5+6+7+12->0+1+0+1->0

8-> 0+10+11+12->1+1+1+1->0

第2位的值是不正确的,因此发送的12位值应该是

0×A4F, 原先的8位数据值是10101111,用十六进值表示应该是0×AF.

11．位流10011101使用标准的CRC使用标准的CRC发送。生成多项式是x^3+1。说明实际发送的位串。假定左起第3位在传输期间变反了。说明该差错在接收方是怎样可以被检测到的。

解答：位流是10011101，生成多项式是1001，在位流后面附加3个0变成10011101001，用1001去除10011101000的余数是100。因此实际发送的位串是10011101100，收到的第3位变反了的位流是10111101100。用1001去除这个位串产生余数100。由于余数不是0，接收方就知道传输过程中发生了差错，可以请求重传。

12．你能想出在什么环境下开环协议（例如海明码）较之反馈型协议（依赖重传）更为可取 吗？

解答：如果传播延迟很长，例如在探测火星或金星的情况下，需要采用前向错误纠正方法。还有在某些军事环境中，接收方不想暴露自己的地理位置，所以不宜发送。如果错误率足够地低，纠错码管用（冗余位串不是很长，又能纠正所有的错误），前向纠错协议也可能是比较简单的。

13．一个上层信息被分成10帧，每帧无损坏地到达目的地的可能性是80%。如果数据链路协议不进行差错控制，那么这一信息平均要发送多少次才能完整地到达接收方？

解答：由于每一帧有0.8的概率到达，整个信息到达的概率是$p=0.8^{10}\approx0.107$。为使信息完整地到达接收方，发送　一次成功的概率是p

二次成功的概率是（1-p）p

三次成功的概率是$（1-p）^2p$

.

.

.

i次成功的概率是（1-p）$^{i-1}$p

因此平均发送次数等于：

$$E=1\times p+2\times(1-p)p+3\times(1-p)^2p+\cdots+i(1-p)^{i-1}p+\cdots$$

$$=\sum_{i=1}^{\infty} i\,p\,(1-p)^{i-1}=p\sum_{i=1}^{\infty} i\,(1-p)^{i-1}$$

为化简这个式子，利用公式：

$$s=\sum_{i=1}^{\infty} a^i=\frac{a}{1-a}$$

$$s'=\sum_{i=1}^{\infty} i\,a^{i-1}=\frac{1}{(1-a)^2}$$

令 $(1-p)=a$

$$E=p\sum_{i=1}^{\infty} i\,a^{i-1}=p\frac{1}{(1-a)^2}=p\frac{1}{[1-(1-p)]^2}$$

$$=p\frac{1}{p^2}=\frac{1}{p}$$

$$E=\frac{1}{0.107}\approx 9.3$$

因此，平均要发送9.3次才能完整地到达目的地。

14．检错的一个方法是按n行、每行k位的块传输数据，并在每行每列增加奇偶位。这种方法能检测出所有单个位错误吗？2位的错误呢？3位的错误呢？

解答：单个错误将引起水平和垂直奇偶检查都显示出错。两个错误也容易被检测到。三个错误也容易被检测到，而不管它们是在同一行（列），两行（列），或在三个不同的行（列）。

15．一个n行和k列的位块使用水平和垂直奇偶位来进行错误检测。假设由于传输错误，有4位反了，列出错误检测不出来的概率的表达式。

解答：让我们用n行k列的矩阵来描述错误图案，在该矩阵中，正确的位用0表示，不正确的位用1表示。由于共有4个传输错误，每个可能的错误矩阵中都有4个1。总共有多少个错误矩阵呢？有nk种放置第1个1的方法，（nk-1）种选择第2个1的位置的方法，（nk-2）种选择第3个1的位置的方法，（nk-3）种选择第4个1的位置的方法；因此错误矩阵的数目是nk（nk-1）（nk-2）（nk-3）。仅当4个1都处在一个矩形的顶点时才会检验不出传输错误。使用笛卡尔坐标，每一位都用在第一象限中的坐标（x，y）表示，这里0≤x<k ，0≤y<n. 那么，每一位的x坐标的可能值是0，1，2，…，k-2，k-1；y坐标的可能值是0，1，2，…，n-2，n-1。假定矩形最靠近原点（即矩形的左下方顶点）的位坐标是（p，q），那么对应于顶点（p，q）的合法矩形的个数是（k-p-1）（n-q-1）。因此，对于所有可能的p和q，可以得到的矩形的总数是：

$$\sum_{p=0}^{k-2}\sum_{q=0}^{n-2}(k-p-1)(n-q-1)$$

所以未被检测出来的错误的概率是：

$$\frac{\sum_{p=0}^{k-2}\sum_{q=0}^{n-2}(k-p-1)(n-q-1)}{nk(nk-1)(nk-2)(nk-3)}$$

16．用发生器多项式x^3+1去除x^7+x^5+1，所得的余数是多少？

解答：

```
          1 0 1 1 0
        ------------
1 0 0 1 | 1 0 1 0 0 0 0 1
          1 0 0 1
          -------
            1 1 0 0
            1 0 0 1
            -------
              1 0 1 0
              1 0 0 1
              -------
                  1 1 1
```

所以，所得的余数是x^2+x+1 。

17．数据链路协议几乎总是把CRC放在尾部，而不是放在头部，为什么？

解答：CRC是在发送期间进行计算的。一旦把最后一位数据送上外出线路，就立即把CRC编码附加在输出流的后面发出。如果把CRC放在帧的头部，那么就要在发送之前把整个帧先检查一遍来计算CRC。这样每个字节都要处理两遍，第一遍是为了计算检验码，第

二遍是为了发送。把CRC放在尾部就可以把处理时间减半。

18．一个信道的比特率是4kbps，传播延迟为20毫秒，那么帧的大小在什么范围内，停-等协议才有至少50%的效率？

解答：当发送一帧的时间等于信道的传播延迟的2倍时，信道利用率是50%。或者说，当发送一帧的时间等于来回路程的传播延迟时，效率将是50%。

20毫秒╳2=40毫秒

现在发送速率是每秒4000位，即发送一位需0.25毫秒

40毫秒÷0.25毫秒/位=160位

答：帧大于160位停-等协议才有至少50%的效率。

19．一个3000公里长的T1干线被用来传送采取后退n帧错误重传滑动窗口协议的长度都是64字节的数据链路帧。如果传播速度是每公里6微妙，那么序列号应该是多少位？

解答：为了有效运行，序列空间（实际上就是发送窗口大小）必须足够地大，以允许发送方在收到第1个确认应答之前可以不断发送。

6×3000=18000（微秒）

传播时间是18000微妙，即18毫秒。

在T1速率，即

$8\times24\times8000=1.536\times10^6$bps （不包括每个物理帧中的1个帧位）。

发送64字节的帧需化时间：

64×8÷1.536≈333 （微秒），即0.333毫秒，约等于0.3毫秒。

因此，第一个帧从开始发送起，18.3毫秒后完全到达接收方。确认应答又化了回程18毫秒加上很少的（可以忽略）发送时间，就可以完全收到。

这样，加在一起的总的时间是36.3毫秒。发送方应该有足够的窗口空间，从而能够连续发送36.3毫秒。

36.3÷0.3=121

也就是说，为充满管道需要121帧，因此序列号应该是7位。

20．在后退n帧错误重传的滑动窗口协议中，需要检查条件（在正确收到1帧后）ack_expected≤r.ack<next_frame_to_send的真伪。这里的ack_expected表示本站作为发送方期待接收的确认应答号，r.ack是本站作为发送方已收到的确认应答号，next_frame_to_send是本站作为发送方下一个要发送的号码。如果把这里的检查条件改成ack_expected≤r.ack≤next_frame_to_send，那么，这个改变会对该协议的正确性或效率有什么样的影响呢？请解释你的答案。

解答：改变检查条件后，协议将变得不正确。我们假定使用3位序列号，考虑下列协议运行过程：

A站刚发出7号帧；B站接收到这个帧，并发出捎带应答ack。A站收到ack，并发送0至6号帧。假定所有这些帧都在传输过程中丢失了。B站超时，重发它的当前帧，捎带确认号

为7号。考察A站在r.ack=7到达时的情况，关键变量是ack_expected=0，r.ack=7，next_frame_to_send=7。修改后的检查条件将被置成“真”，不会报告已发现的丢失帧错误，误认为丢失了的帧已被确认。在另一方面，如果仍使用原先的检查条件，就能报告丢失帧的错误。因此，我们得到结论：为保证协议的正确性，已接收的确认应答号必须小于下一个要发送的号码。

21．假设有一个滑动窗口协议使用许多位作为序列号，使得在接收端能分辨出序列中预期新发来的帧编号和那些重发射的老的帧编号。那么，4个窗口边界及窗口大小必须保持什么样的关系？

解答：问题的关键在于，接收方向前移动其窗口后，新的有效序列号范围不与原先的有效序列号范围重迭。为保证不发生重迭，最大的窗口尺寸应该不超过序列号范围的一半。如图3-3所示，如果用4位来表示序列号，其范围是0~15。任何时刻，只允许有8个未确认帧。这样一来，如果接收过程刚刚接受了0~7号帧，向前移动了窗口，允许进行第8至第15号帧的接收，那么就能分辨出后继帧是重发帧（由于传输过程中确认帧的丢失，或发送方超时重传）0~7，还是新帧8~15。

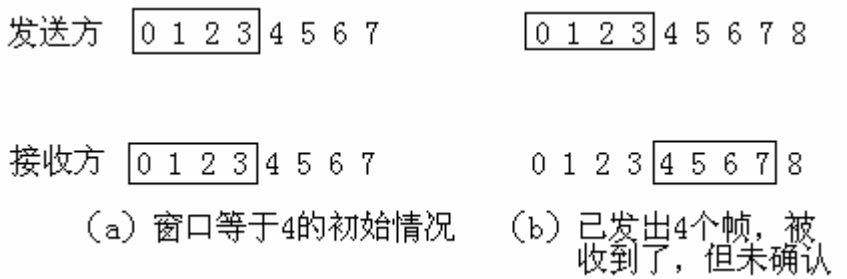


图 3-3 习题 21 插图

一般说来，窗口大小为（MAX__SEQ+1）/ 2。由图中给出的例子可以看出，如果发送方的窗口用（S_L，S_U）表示，接收方的窗口用（R_L，R_U）表示，并假定窗口是W，那么，

$0 \leqslant S_U - S_L + 1 \leqslant W$

$R_U - R_L + 1 = W$

$S_L \leqslant R_L \leqslant S_U + 1$

22．在使用选择性重传的滑动窗口协议中，当一个数据帧到达时，要检查其序列号是否不同于所期待接收的号码，同时要检查布尔量NONAK是否为真。这里的NONAK表示还没有发送过NAK。如果这两个条件都成立，就发出一个NAK，否则就要启动一个辅助计时器。假定省去“否则”子句，会对协议的正确性有什么样的影响？

解答：可能导致死锁。假定有一批的帧正确到达，并被接收。然后，接收方将会向前移动其窗口。现在假定所有的确认都丢失了，发送方最终会产生超时事件，并且再次发送第一帧，接收方将发送一个NAK。然后NONAK被置成伪。假定NAK也被丢失了，那么从这时候开始，发送方不断发送已经被接收方接受了的帧。接收方只是忽略这些帧，但由于NONAK为伪，所以不会再发送NAK，从而产生死锁。如果设置辅助计数器（实现“否则”

子句），超时后重发NAK，终究会使双方重新获得同步。

23．在一个实现采取选择性重传的滑动窗口协议的程序代码的接近结尾处，有一个由3条语句组成的while循环：

```
while(between(ack_expected, r.ack, next_frame_to_send))
    {nbuffered=nbuffered-1;     /*处理捎带确认*/
     stop_timer(ack_expected%NR_BUFS);  /*帧完整到达*/
     inc(ack_expected); /*将发送方窗口的低端向前推进*/
    }
```

这里的nbuffered表示发送缓存中保留的输出帧的数目，ack_expected表示下一个期待接收的确认帧的号码。如果把这一段程序代码删除，这会影响协议的正确性吗？还是仅影响性能？请解释你的回答。

解答：删除这段程序会影响程序的正确性，导致死锁（也可称活锁）。因为这段程序负责处理接收到的确认帧，没有这一段程序，发送方会一直保持超时条件，从而使得协议的运行不能向前进展。

24．在使用1位序列号并且做肯定应答的停止等待式ARQ协议中，发送方有可能在定时器已在运行的情况下启动定时器吗？如果可能，说明是如何发生的。如果不可能，说明为什么。

解答：有可能。假定发送方发送了一个帧，但应答帧在途中被破坏，发送方收到时识别不了。在这种情况下，发送方第2次发送该帧，并启动定时器，此时上一次启动的定时器仍在运行。

25．在一个实现采取选择性重传的滑动窗口协议的程序代码中，如果把负责处理错误检验码的那部分程序删除，会影响协议的运行吗？

解答：将会取消否定确认的功能，因此将回到超时重传操作。虽然性能会有所减退，但不会影响数据传输服务的正确性。NAK不是必须的。

26．在一个实现采取选择性重传的滑动窗口协议的程序代码中，在处理输入帧的部分有下列语句：

```
if((r.kind=     =nak)&&between(ack_expected,     (r.ack+1)%(MAX_SEQ+1),
next_frame_to_send))
  send_frame(data, (r.ack+1)%(MAX_SEQ+1), frame_expected, out_buf);
```

如果到达的帧是一个NAK，且另一个条件也满足，就涉及此部分程序。是给出某种情况，说明另一个条件也是重要的。

解答：这里要求 r.ack+1<next_frame_to_send。考虑下列操作细节：

A站发送0号帧给B站。B站收到这个帧，并发送ACK帧，但ACK被传丢了。A站发生超时，重发0号帧，但B站现在期待接收1号帧，因此它发送NAK，否定收到的0号帧。显然，现在A站最好不重发0号帧。由于条件r.ack+1<next_frame_to_send不成立，所以用不着选择

性重传0号帧，可以继续向前推进传送1号帧。这个例子就说明了这段程序中另一个条件，即r.ack+1<next_frame_to_send，也是重要的。

27．假定你正在为一条线路编写数据链路层软件，该线路被用来发送数据给你，而不是从你发出数据。另一端使用HDLC，序列号采用3位，窗口大小是7。你打算缓存所有可能的未确认序列帧，以提高效率，但不允许修改发送方的软件。是否可以使接收方窗口大于1并仍保证协议不会失败？如果可以，能够安全使用的最大窗口值是多少？

解答：不可以。最大接收窗口的大小就是1。现在假定该接收窗口值变为2。开始发送方发送0至6号帧，所有7个帧都被收到，并作了确认，但确认被丢失。现在接收方准备接受7号和0号帧。当重发的0号帧到达接收方时，它将被缓存保留，接收方确认6号帧。当7号帧到来时，接收方将把7号帧和缓存的0号帧传递给主机，导致协议错误。因此，能够安全使用的最大窗口值就是1。

28．假定在一条无错线路上运行采用选择性重传的滑动窗口协议，线路速率是1Mbps，最大帧长度是1000比特。每一秒钟产生一个新帧。超时间隔是10毫秒。如果删除ACK超时机制，将会发生不必要的超时事件。平均每个报文要传送多少次？

解答：发送1位用时间1微妙，发送1000比特的最长帧化时间1毫秒。由于超时间隔是10毫秒，而1秒钟才能产生一个新的数据帧，所以超时是不可避免的。假定A站向B站发送一个帧，正确到达接收方，但较长时间无反向交通。不久，A站发生超时事件，导致重发已发过的一帧。B站发现收到的帧的序列号错误，因为该序列号小于所期待接收的序列号。因此B站将发送一个NAK，该NAK会携带一个确认号，导致不再重发该帧。结果是，每个帧都被发送两次。

29．在一个采用选择性重传的滑动窗口协议中，MaxSeq=2^n-1。为了有效地使用n个帧头位，显然这是我们所希望的。如果让MaxSeq=4，协议还能正确地工作吗？

解答：不能，协议的运行将会失败。当MaxSeq=4，序列号的模数n=4+1=5，窗口大小将等于：

NrBufs≤5/2=2.5, 即得到，NrBufs=2

因此，在该协议中，偶数序号使用缓冲区0，奇数序号使用缓冲区1。这种映射意味着帧4和0将使用同一缓冲区。假定0至3号帧都正确收到了，并且都确认应答了。如果随后的4号帧丢失，且下一个0号帧收到了，新的0号帧将被放到缓冲区0中，变量arrived[0]被置成“真”。这样，一个失序帧将被投递给主机。事实上，采用选择性重传的滑动窗口协议需要MaxSeq 是奇数才能正确地工作。然而其它的滑动窗口协议的实现并不具有这一性质。

30．在一个1Mbps的卫星信道上发送1000比特长的帧。确认总是捎带在数据帧中。帧头很短，使用3位的序列号。对以下协议而言，可以取得的最大信道利用率是多少？

（a）停-等协议
（b）回退N滑动窗口协议
（c）选择性重传滑动窗口协议

解答：对应三种协议的窗口大小值分别是1、7和4。

使用卫星信道端到端的传输延迟是270毫秒，以1Mbps发送，1000比特长的帧的发送时间是1毫秒。我们用t=0表示传输开始时间，那么在t=1毫秒时，第一帧发送完毕。t=271毫秒，第一帧完全到达接收方。t=272毫秒时，对第一个帧的确认帧发送完毕。t=542毫秒时带有确认的帧完全到达发送方。因此周期是542毫秒。如果在542毫秒内可以发送k个帧（每个帧发送用1毫秒时间），则信道利用率是k/542，因此，

（a）k=1，最大信道利用率=1/542=0.18%
（b）k=7，最大信道利用率=7/542=1.29%
（c）k=4，最大信道利用率=4/542=0.74%

31．使用选择性重传滑动窗口协议，在有重负载的50kbps的卫星信道上，传输包括40位的头部和3960个数据位的数据帧，ACK帧从未发生，NAK帧长40位，数据帧的错误率是1%，NAK的传输错误率可忽略不计，序列号长度是8位。试计算化在开销（头和重传）上的带宽的比例。

解答：使用选择性重传滑动窗口协议，序列号长度是8位。窗口大小为$2^8 \div 2=128$。卫星信道端到端的传输延迟是270毫秒。以50kbps发送，4000比特（3960+40=4000）长的数据帧的发送时间是0.02×4000=80毫秒。我们用t=0表示传输开始时间，那么，在t=80毫秒时，第一帧发送完毕。t=270+80=350毫秒时，第一帧完全到达接收方。t=350+80=430毫秒时，对第一帧做捎带确认的反向数据帧可能发送完毕。t=430+270=700毫秒时，带有确认的反向数据帧完全到达发送方。因此，周期是700毫秒。在700毫秒内可以发送128帧，80毫秒×128=1024毫秒。显然，1024毫秒>700毫秒意味着传输管道总是充满的。每个帧重传的概率是0.01，对于3960个数据位，头位开销40位，平均重传位数是4000×0.01=40位，传送NAK的平均位数是40×1/100=0.40位，所以每3960个数据位的总开销是80.4位。因此开销所占带宽比例等于80.4÷（3960+80.4）≈1.99%。

32．使用一个64kbps的无错卫星通道发送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。对于窗口大小1、7、15和127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270毫秒，以64kbps发送，512字节长的数据帧占据通道的时间是$512\times8\div64000=64\times10^{-3}$秒，即64毫秒。我们用t=0表示传输开始时间，那么在t=64毫秒时，第一帧发送完毕，t=64+270=334毫秒时，第一帧完全到达接收方，并开始返回很短的确认帧（发射时间忽略不计），t=334+270=604毫秒，确认帧完全到达发送方。因此，周期等于604毫秒，我们需要窗口大小为604÷64≈9个帧才能保持通道不空。

对于窗口值1，每604毫秒可发送4096位，吞吐率为4096÷0.604≈6781bps，约为6.8kbps。
对于窗口值7，吞吐率为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。

33．一条100公里长的电缆以T1数据速率运行，在电缆中的传播速率是光速的2/3，在该电缆中可以充填多少位？

解答：在该电缆中的传播速度是每秒200000公里，即每毫秒200公里，因此，100公里的电缆将会在0.5毫秒时间内填满。T1速率125微妙传送一个193位的帧，0.5毫秒（即500微妙）可传送4个T1的帧，193位×4=772位。所以，在该电缆中可充填772位。

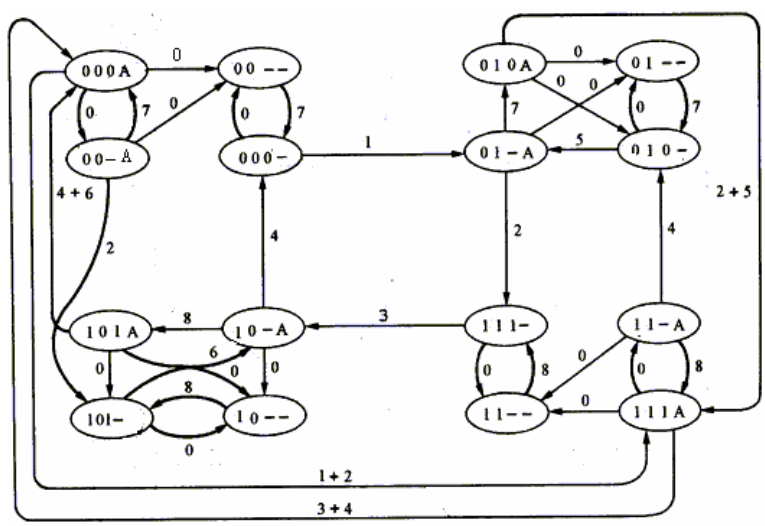
34．对于使用1位序列号窗口大小为1的双向滑动窗口协议使用有限状态机模型模拟，每个机器有多少个状态？对于通信通道有多少个状态？整个系统（两个机器和通道）有多少个状态？忽略检验和错误。

解答： 每个机器有两个主要变量：next_frame_to_send和frame_expected。每个变量都可以取值0或1。因此每个机器处在4个可能的状态之一。在通道上的一个报文包含被发送的帧的序列号以及被ACK的（确认）的帧的序列号。因此存在4种类型的报文。通道在任一方向上都可能包含0个或一个报文。因此通道中有0个报文是一个状态，有一个报文是8个状态，有两个报文（每个方向一个报文）是16个状态。1+8+16=25，因此通道有25个可能的状态。

$4\times4\times25=400$

所以整个系统有400个可能的状态。

35．图3-4是一个协议的有限状态机模型。我们用通信的两个协议机的状态和2条信道的状态的合成状态来描述该协议。正向信道具有3种状态：帧0，帧1或空；而反向信道具有2种状态：A或空。每种状态由4个字符XYZW标识。这里的X是0或1，对应着发送方试图发送或已发送但未得到确认应答的帧；Y也是0或1，对应着接收方希望收到的帧；Z是0，1或空（-），对应着正向信道的状态；W是A或空（-），对应着反向信道的状态。表3-1示出了变迁的定义。如果必须两个事件同时发生，则相关的变迁用两个数字相加的标记来表示，例如，在状态（000A）和状态（111A）之间的变迁在图中标记为1+2。



(a)

(000–), (01–A), (010A), (111A), (11–A), (010–), (01–A), (111–)

(b)

图 3-4　习题 35 插图 1

在图3-4（a）中存在着导致协议失败的路径。图3-4（b）给出了引起协议失败的一个状态序列。在此序列的第四和第六个状态上，发送过程改变了状态，这表明发送过程从上面的网络层取得了一个新分组，而接收过程却没有改变状态，也就是说，接收方没有向上面的网络层递交任何分组。

现在假定此时的全双工通道不会丢失帧。还可能发生协议失败吗？

表3-1　变迁的定义

变迁	谁运行？	接受的帧	发送的帧	至网络层吗？
0	-	（帧丢失）		-
1	接收方	0	A	是
2	发送方	A	1	-
3	接收方	1	A	是
4	发送方	A	0	-
5	接收方	0	A	否
6	接收方	1	A	否
7	发送方	（超时）	0	-
8	发送方	（超时）	1	-

解答：在全双工通道不会丢失帧的情况下，图3-4应该变成如图3-5所示的那样。也就是说，新图基本上和原图一样，但是原图中的状态（00--）、（00-A）、（010-）、（11-A）、（01--）、（11--）、（101-）和（10--）都消失了。协议的失败已不再可能。值得注意的是，当数据帧和确认帧同时出现在信道上时，需要做特别的处理。接收过程不能自己单独把数据帧拿走，因为这样做会引起在信道上有两个确认帧同时存在，这在我们的模型中是不允许的。类似地，发送过程也不能自己单独取走确认帧，因为这样做的结果就会在第一帧被接受之前又发送出第二个数据帧。这就要求2个事件一起发生，才能保持协议的正确运行。例如，事件1和事件2一起发生，在状态000A和111A之间进行变迁，在图中标记为1+2。

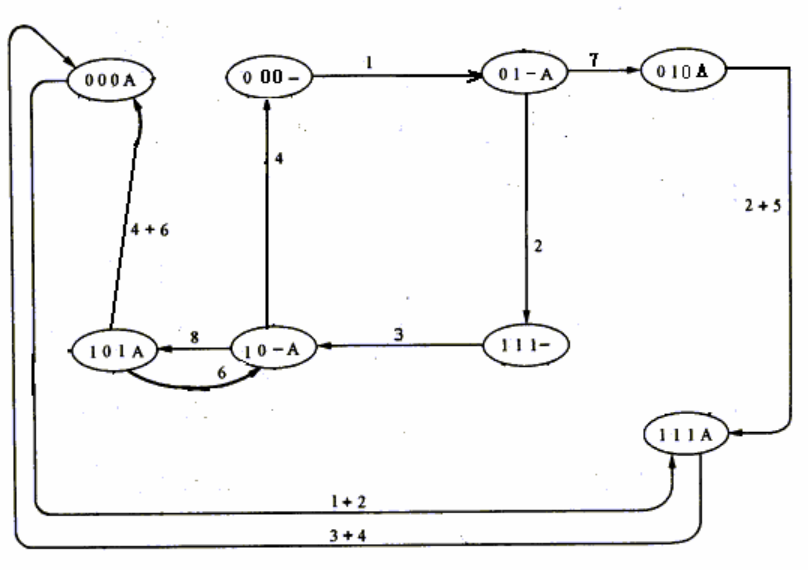


图 3-5　习题 35 插图 2

36．给出对应于图3-6的状态序列（000）、（01A）、（01-）、（010）、（01A）的如图3-7表示的Petri网激发序列。请用文字解释所代表的序列。

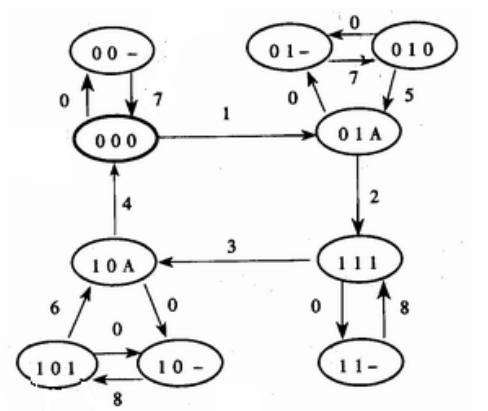


图 3-6　习题 36 插图 1

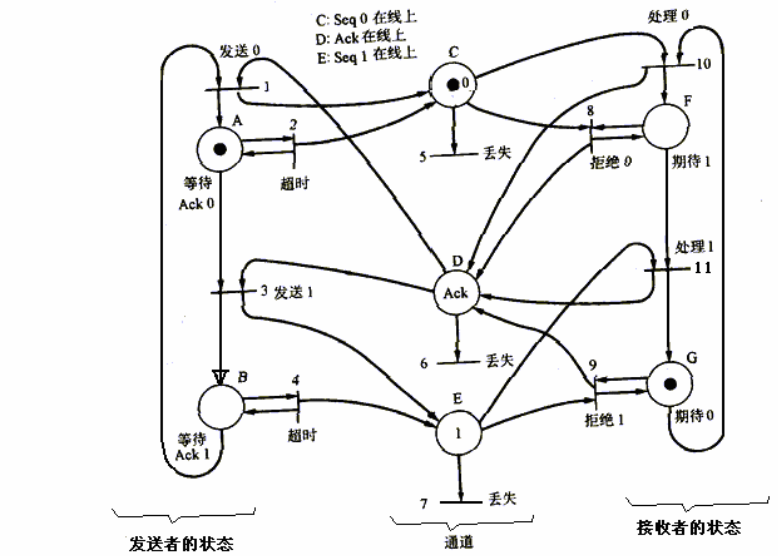


图 3-7　习题 36 插图 2

解答：在图3-6中，每种状态由3个字符XYZ标识，这里的X是0或1，对应着发送方试图发送或已发送但未得到确认应答的帧，Y也是0或1，对应着接收方希望收到的帧，Z是0、1、A（确认）或空（-），对应通道的4钟状态。因而，

（000）→ (01A) → (01-) → (010) → (01A) 对应Petri网中的变迁10，6，2，8。这里的10表示接受一个0号帧，6表示接收方发出的ACK帧在通道上丢失，2表示发送方超时而重发0号帧，8表示接收方拒收0号帧并再次发送ACK帧。

37．给出传输规则AC→B，B→AC，CD→E和E→CD，画出所描述的Petri网。从Petri网画出从初始状态ACD可达的有限状态图。这些变迁规则模拟了哪个著名的计算机科学概念？

解答：Petri网如图3-8所示。状态图如图3-9所示。所模拟的系统是互斥机制。B和E是关键的部分，它们不能同时处于活动状态，即状态BE是不允许的。位置C表示一个信号灯，它可以被A或D获取，但不能被A和D一起获取。

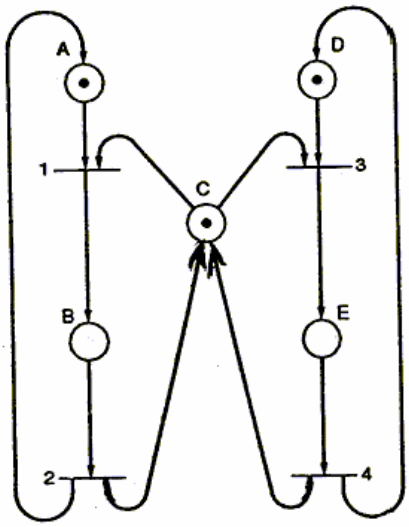


图 3-8 习题 37 插图 1

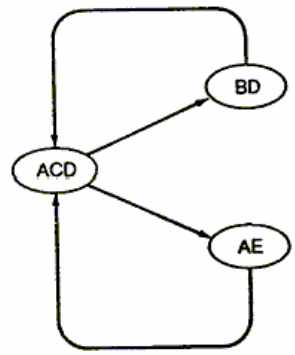


图 3-9 习题 37 插图 2

38．PPP是以HDLC为基础的，HDLC使用位充填防止在有效载荷内偶尔出现的标志字节产生混淆。给出至少一个理由，说明PPP为什么使用字符充填来代替位充填。

解答：PPP被明确地设计成是以软件形式实现的，而不像HDLC那样几乎总是以硬件形式实现。对于软件实现，完全用字节操作要比用单个位操作简单得多。此外，PPP被设计成跟调制解调器一道使用，而调制解调器是以1个字节为单元而不是以1个比特为单元接受和发送数据的。

39．在使用PPP发送一个IP分组时，最小的开销是多少？仅考虑由PPP本身所引入的开销，而不计IP头部的开销。

解答：图3-10示出了PPP的帧格式。

由于在缺省配置下，地址和控制字段总是常数，因此LCP（链路控制协议）为这二部分提供了必要的机制，可以协商选项，允许省略掉这2个字段，从而在每帧上节省2个字节。协议段缺省大小为2字节，但在使用LCP时，可以变成1字节。

字节 1	1	1	1或2	可变	2或4	1
01111110	11111111	00000011	协议	载荷	检验和	01111110
标志	地址	控制				标志

图 3-10 习题 39 插图

在最小开销条件下，每个帧有两个标志字节，一个协议字节和两个检验和字节，这样，每个帧共有5个开销字节。

40．详细说明HDLC是如何在不满足W≤n/2的条件下解决重发帧与新收到帧之间的编号混淆问题的？

解答：在作为数据链路层协议的HDLC中，传输媒体的特性是可断定的。网络中相邻节点之间的媒体本身不会引起帧的失序，媒体本身也不会产生重发的帧。响应时间的最大极限可以精确地计算，从而可以设置超时值进行最佳的错误恢复。由于一方面发送方接收对错误的响应，一方面链路上顺序自然得到维持，接收方仅接收按顺序到来的帧，所以在图3-6中，可以不考虑K，只考虑R+1，故只要使L和R+1之间的模n的编号在同一周期内即可。设以模n编号的0左边有n_1个帧，右边有n_2个帧。

$L=n-n_1$

$R+1=n_2$

要求$L>R+1$

即$n-n_1>n_2$

$n_1+n_2+1\leqslant n$

由于$n_1+n_2+1\leqslant w+1$(即从L到R+1的宽度)

所以只要满足$w+1\leqslant n$就可以了。

也就是$w\leqslant n-1$。

41．一条信息被分成很多块时，需要在每一块上附加一些比特来提供诸如同步、错误控制及地址的功能，假设每个块包含N比特（其中有H个附加比特），线路的比特错误率为ε，并且出错的块必须重发。现在要发送一条有1352个比特的信息。假设附加的比特数H是固定的，不管块的大小，都等于168比特，且有$\varepsilon=10^{-4}$，试确定能使整个传送比特数（包括重传比特）的平均数最小的最佳块长度N。当$\varepsilon=10^{-3}$时，结果会有什么不同？

解答：传送一块的出错概率是$p=1-(1-\varepsilon)^N$

每块需要传送的平均次数是:

$$T=1+\sum_{i=1}^{\infty} ip^i(1-p)=1+\frac{p}{1-p}=\frac{1}{1-p}$$

由于信息长度等于1352比特，则信息可分成1352/（N-168）块。

那么，总共传送的平均总次数是：

$$\frac{1352}{(N-168)}\cdot\frac{1}{1-p}$$

所以总共传送的比特数是：

$$G=\frac{1352}{(N-168)}\cdot\frac{1}{1-p}\cdot N$$

用$p=1-(1-\varepsilon)^N$代入，得到

$$G = \frac{1352}{(1-\varepsilon)^N} \cdot \frac{N}{(N-168)}$$

当 ε 《 1 时，（1- ε ）^{N}≈1- ε N，

$$\therefore \quad G = \frac{1352}{1-\varepsilon N} \cdot \frac{N}{(N-168)}$$

令 $\frac{dG}{dN} = 0$

得到 ε N^2=168

所以，$N = \sqrt{\frac{168}{\varepsilon}}$

当 ε =10^{-4}时，N≈1296

当 ε =10^{-3}时，N≈410。

42．在大多数网络中，数据链路层通过请求重传损坏帧来处理传输错误。如果一个帧被损坏的概率为p，在确认帧永远不会被丢失的情况下发送一帧所需要的平均传输次数是多少？

解答：一个帧需要传输k次的概率p_k是开头k-1次传输尝试失败的概率p^{k-1}乘以第k次传输成功的概率（1-p）。因此，平均传输次数是：

$$\sum_{k=1}^{\infty} kp_k = \sum_{k=1}^{\infty} k(1-p)p^{k-1}$$

$$= \frac{1-p}{p} \sum_{k=1}^{\infty} kp^k = \frac{1-p}{p} \cdot \frac{p}{(1-p)^2}$$

$$= \frac{1}{1-p}$$

43. 一个报文由100个8比特字符组成，使用下列传输控制方案在一条数据链路上传输，需要多少附加的比特？

（a）异步方式，每个字符使用一个起始位和两个停止位，每个报文使用一个帧起始字符和一个帧结束字符；

（b）同步方式，每个报文使用两个同步字符、一个帧起始字符和一个帧结束字符。

解答：

（a）异步方式，每个字符中的附加位数等于1+2=3，

（3×100）+ 2×（3+8）= 322

∴传输一个报文需要322个附加的比特

同步方式，每个报文附加两个同步字符、一个帧起始字符和一个帧结束字符。

4×8 = 32

∴传输一个报文需要32个附加的比特

44. 一块数据通过一条串行数据链路以异步方式传输。如果接收方可提供19.2KHZ的时钟，试计算在下列数据传输速率条件下的时钟速率比，并估算以位周期的百分比表示的从正常位单元中心的最坏情况偏移。

（a）1200bps

（b）2400bps

（a）9600bps

解答：接收方时钟信号（RxC）的运行相对于输入信号（RxD）是异步的，两种信号的相对位置可以在单个接收方时钟周期内的任何地方。从正常位单元中心的最坏情况偏移大约是接收方时钟的一个周期，因此：

（a）在1200bps数据速率条件下，最大接收方时钟比率可以是×16，因此最大偏移是6.25%。

（b）在2400bps数据速率条件下，最大接收方时钟比率可以是×8，因此最大偏移是12.5%。

（c）在9600bps数据速率条件下，最大接收方时钟比率可以是×2，因此最大偏移是50%。

显然，最后一种情况是不可接收的。对于低质量的线路，特别是具有过量延迟失真的线路，甚至第二种情况也是不可靠的。 出于这种原因，应尽可能使用×16的时钟速率比。

45. 使用CRC做错误检测，传送8位的帧序列。生成多项式是11001。试举一个例子说明：

（a）FCS生成过程；

（b）FCS检查过程。

解答：

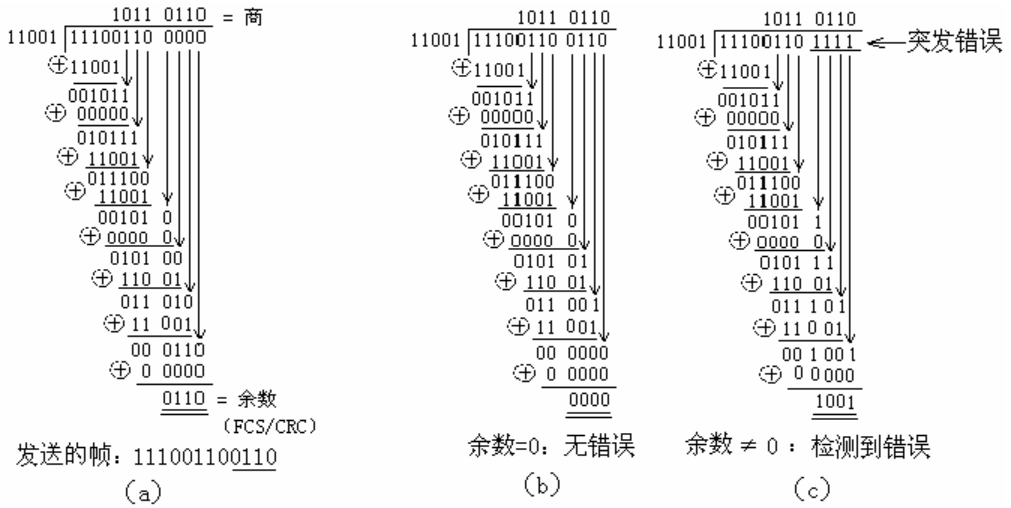


图 3-11　习题 45 插图

假定为报文块11100110生成FCS。首先，附加4个零到报文块，这等效于将报文块乘上2^4，因为FCS是4位。然后再除以用二进制表示的生成多项式（11001）。注意在模2除操作过程中应执行一系列的异或运算。除法运算的结果所产生的4位余数（0110）就是FCS（帧检验序列）。发送时，FCS将被附加到原始报文块的尾部（参见图3-11（a））。

在接收端，收到的完全位序列用跟发送方相同的生成多项式去除。如果传输过程中无错误发生，余数将是零（参见图3-11（b））。如果在发送的位序列的尾部发生4位的突发性错误，余数将不是零，表明有传输错误（参见图3-11（c））。

46. 使用BSC协议控制在一条多点数据链路上在一台计算机（主站）和10个块方式终端（次站）之间的报文流。链路数据速率（R）是10Kbps，一个报文的平均长度（N_i）是1000位。如果一个轮询报文及相关的ACK是30位，并且处理这些报文的总时间是1毫秒，确定在下列产生报文的平均速率下每个报文被轮询的平均时间。

（a）每分钟一个报文

（b）每秒钟6个报文

忽略链路的位错率和信号传播延迟时间。

解答：一般情况下，如果链路上次站的数目为N，那么，在不发送任何报文的情况下，轮询所有次站所需要的最短时间是轮询单个次站所化时间的N倍。当有报文发送时，轮询所有次站的平均时间增加，并且跟产生报文的平均速率有关。当产生报文的平均速率接近链路位速率时，轮询所有次站的时间最长。

轮询所有次站的平均时间可以表示为：

$$T_{avr} = \frac{T_{min}}{1 - Mr\ T_{ix}}$$

这里的T_{min}是轮询所有次站的最少时间，Mr是产生报文的平均速率，T_{ix}是发送一个平

均大小的报文的时间。

在本题中，发送一个平均报文的时间（T_{ix}）是：

$N_i/R = 1000/10^4 = 100$毫秒

发送一个轮询和ACK的时间是：$30 / 10^4 = 3$毫秒

轮询单个次站的时间是：3+1 = 4毫秒

轮询所有次站的最少时间是：$T_{min} = 10\times4=40$毫秒

这里的T_{min}是轮询所有次站的最少时间，Mr是产生报文的平均速率，T_{ix}是发送一个平均大小的报文的时间。

（a）Mr等于每分钟一个报文，即每毫秒10^{-3}/60个报文。因此，

$$T_{avr} = \frac{40}{1 - \frac{10^{-3}}{60} \times 100} = 40 \text{ 毫秒}$$

（b）Mr 等于每秒钟六个报文，即每毫秒6×10^{-3}个报文。因此，

$$T_{avr} = \frac{40}{1 - 6 \times 10^{-3} \times 100} = \frac{40}{0.4} = 100 \text{ 毫秒}$$

47. 考虑在一条20公里长的点到点光纤链路上运行的ARQ算法

（a）假定光在光纤中的传播速度是2×10^8米/秒，试计算该链路的传播延迟。

解答：传播延迟=20×10^3米÷（2×10^8米/秒）=100微妙

（b）为该ARQ建议一个适当的超时值。

解答：往返时间大约为200微妙。可以把超时值设置成该时间长度的2倍，即0.4毫秒。取决于在实际的RTT中的变化量额，有时候取小一些的值（但大于0.2毫秒）也许更合理。

（c）按照给出的这个超时值实现ARQ算法，为什么该ARQ算法在运行过程中还可能超时而重传帧呢？

解答：前面传播延迟的计算没有考虑处理延迟，而在实践中远方结点可能引入处理延迟，即它也许不能够立即回答。

48. 说明两维奇偶检查为接收方提供了足够的信息纠正任意的1位错（假定接收方知道仅有1位错），但所提供的信息不足以纠正任意的2位错。

解答：如果我们知道只有1位错，那么两维奇偶检查能够告诉我们该位在哪1行和哪1列，我们只要把这1位变反就得以纠正了。然而如果在同1行中有两位错，那行奇偶检查依然正确，所有我们能够知道的就是错误位在哪个列。由于确定不了行的位置，也就不能够纠正这两个错误位。

49。考虑一种ARQ协议，它只采用否定应答（NAK），不使用肯定应答（ACK）。试说明在这种情况下需要什么样的超时调度机制。解释为什么通常人们都倾向于采用基于ACK的协议，而不采用基于NAK的协议。

解答：假定只在有失序分组到达的时候才发送NAK。考虑到NAK或被否定应答的分组在传送的过程中可能丢失，接收方必须维护一种RESEND_NAK超时器。然而，如果发送方发送一个分组，然后是一段空闲等待时间，假定这个分组丢失了，那么接收方无法感知该分组的丢失。在这种情况下，为了解决问题，要么让接收方发送ACK，同时发送方维护一种超时器；要么发送方在空闲期间故意发送某种用零填充的失序分组。显然，采用严格的仅否定应答策略时，在一个分组的传输结束后，发送方不能肯定分组是否正确地到达了接收方，需要靠发送填充零的失序分组来解决问题，这显然是一个麻烦的负担。正因为如此，通常人们都倾向于采用基于ACK的协议，而不采用基于NAK的协议。

50．实施流控制的一种方法是使用滑动窗口协议。我们可以让接收方对收到的分组推迟发送ACK，即等到有空闲缓冲区空间存放下一个分组时再发送ACK。在这样做的时候，每个ACK在肯定应答收到上一个分组的同时，也告诉源发方现在有空闲缓冲区空间用以存放下一分组。请解释为什么说以这种方式实现流控制不是一个好主意。

解答：如果接收方推迟发送ACK直到有缓冲区空间为止，它就会冒有这样的风险，即它可能延迟太长的时间，以致发送方不必要地超时，并且重发该分组。

51. 在停-等传输中，假定发送方和接收方在收到一个重复的ACK或数据帧时都立即重传它们的最后一帧；从表面上看，这样的一种策略是合理的，因为收到这样的一个重复帧很可能意味着另一端经历了一个超时事件。

（a）画出时序简图说明，如果第1个数据帧因某种原因重复传输了，而实际上并未发生帧丢失事件，那么会发生什么样的情况。重复事件将持续多长时间？（在实践中人们把这种重复传送现象称着魔术师徒弟的故障）。

解答：如图3-12所示的重复现象持续进行着，直到传输结束为止。

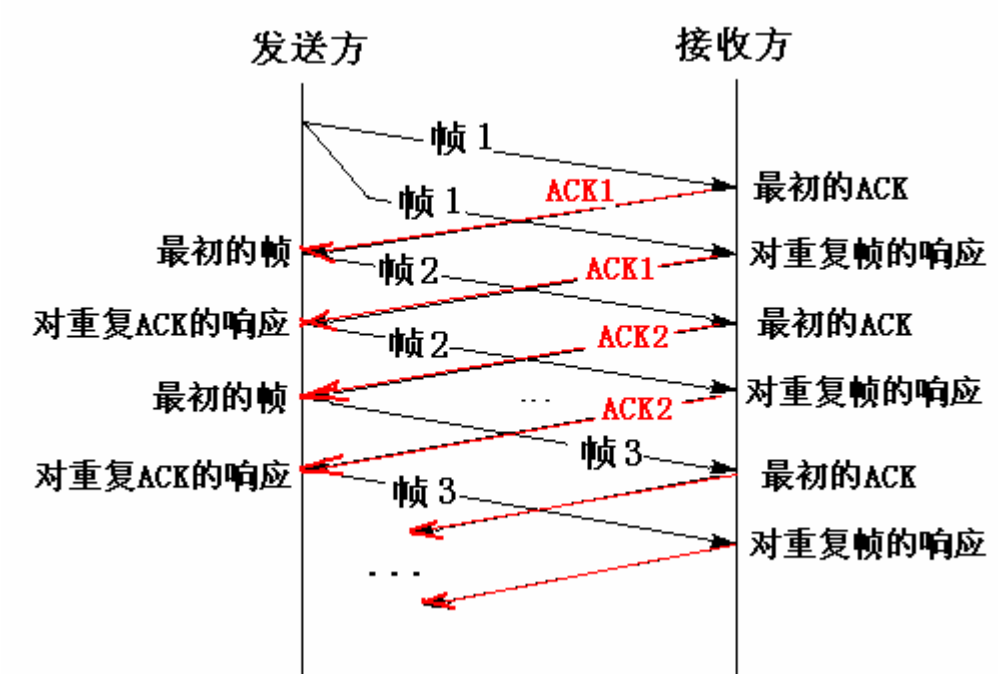


图 3-12　习题 51 插图

（b）假定跟数据一样，如果在超时期内无响应，ACK也重发；再假定两边使用相同的超时间隔。试给出一种可能是合理地触发魔术师徒弟故障的运行条件。

解答：为触发魔术师徒弟现象，重复的数据帧必须与第1个ACK在网络中相遇。如果发送方和接收方都采取超时重发策略，且具有同样的超时间隔，ACK丢失，那么发送方和接收方会在大约相同的时间重发送。这些重发送是否同步到足以在网络中相遇还取决于其它因素。这种超时重发有助于实现某种有节制的延迟，否则主机有可能响应得太慢。通过设定适当的条件，魔术师徒弟现象是可以可靠地产生的。

52. 试给出一种让ACK运载附加信息的流控来增强滑动窗口协议的详细办法。在接收方用完缓冲区空间时，由ACK运载的信息可减少发送窗口尺寸（SWS）。可以借助时序事件说明你的协议。假定初始的SWS和接收窗口尺寸（RWS）都是4，链路速度是即时的（带宽无限大），并且接收方可以用每秒1个的速率释放缓冲区（即接收方是瓶颈）。说明在T=0，T=1，……，T=4时会发生什么样的事件。

解答：下面叙述的是TCP的实际操作：每个ACK都可能包含一个值，发送方可以用该值作为发送窗口的最大值。如果这个值是0，发送方停止发送。当接收缓冲区变得可提供的时候，后来的一个ACK将用一个非0的SWS发送。显然需要提供某种机制来保证这个后来的ACK不会丢失，以避免发送方永远等待。最好每个新的ACK对于SWS的减少不超过1，使得发送最后一帧的号码永远不会减少。

现在假定采用上述协议，我们将得到下列情况：

T=0，发送方发送帧1至帧4，接着相继在反方向传送ACK1，... ，ACK4（在这里ACKn

表示对收到第n帧的应答），分别把SWS设置为3，2，1和0。现在发送方等待SWS>0的条件。

T=1，接收方释放第1个缓冲区；发送ACK4/SWS=1。发送方向前滑动窗口，发送帧5，接收方发送ACK5/SWS=0。

T=2，接收方释放第2个缓冲区；发送ACK5/SWS=1。发送方发送帧6；接收方发送ACK6/SWS=0。

T=3，接收方释放第3个缓冲区；发送ACK6/SWS=1。发送方发送帧7；接收方发送ACK7/SWS=0。

T=4，接收方释放第4个缓冲区；发送ACK7/SWS=1。发送方发送帧8；接收方发送ACK8/SWS=0。

53. 试给出一种把滑动窗口算法跟选择性ACK相结合的协议。你的协议应该有在必要时即时重传的机制，但如果一个帧仅是失序一个或两个号位则不重传。你的协议对于在几个连续的帧丢失时会发生什么样的事件也应该有明确的说明。

解答：下面给出的是一种可能的协议：

如果帧[N]到达，如果它是期待的下一个帧，即NFE=N，那么接收方发送ACK[N]；否则，如果N位于接收窗口之内，那么接收方发送选择性应答SACK[N]。发送方在一个桶内保持若干个N>LAR(接收到的最后一个确认帧号)，等待SACK{N}的到来。注意，每当LAR向前滑动时，桶内所有N≤LAR的帧将被清除。如果该桶包含一个或两个值，这些帧可能是由于失序投递引起的。然而，发送方可以合理地假定，每当有一个N>LAR的帧[N]未被确认，而在桶中有3个后面的SACK时，那么帧[N]丢失了。重传这样的帧也许就可以恢复到正常情况了。几个连续的帧丢失，由于长时间收不到对它们的确认而产生超时，如果窗口足够大，也许还能收到对后续几个帧的SACK，在这种情况下，重传这些丢失的帧也能解决问题。

54. 假定我们运行SWS=5和RWS=3的滑动窗口算法，并且在传输过程中不会发生分组失序的问题。

（a）求MaxSeqNum（可以使用的序列号的个数）的最小值。

你可以假定找出一个最小值MaxSeqNum满足下列条件就可以了：如果DATA[MaxSeqNum]在接收窗口中，DATA[0]再也不会到达。

解答：MaxSeqNum的最小工作值是8。如果DATA[8]在接收窗口中，

-》可能的最早接收窗口是DATA[6]至DATA[8]

-》发送方已经收到了ACK[6]（它应答了序号低于6的分组）

-》DATA[5]已经被投递

但因为SWS=5，DATA[0]是在DATA[5]之前发送

-》根据在传输过程中不会发生分组失序的假定，DATA[0]不可能再发送。

（b）给出一个例子，说明MaxSeqNum-1是不够的。

解答：如果MaxSeqNum=7，那么我们要说明的是，在接收方期待DATA[7]的时候，一个老的DATA[0]仍然可能到达。因为以MaxSeqNum=7为模，7和0是不可区分的，接收方判断不了实际到达的是DATA[7]还是DATA[0]。

-》发送方发送DATA[0]至DATA[4]，它们都到达了。
-》接收方发送ACK[5]作为响应，但它很慢。接收方窗口现在是DATA[5]至DATA[7]。
-》发送方超时，并重发DATA[0]，接收方把该重传的分组作为DATA[7]接收。

（c）给出由SWS和RWS求最小MaxSeqNum的一般规则。

解答：MaxSeqNum≥SWS+RWS。

55. 针对下列两种情况，分别画出SWS=RWS=3的滑动窗口算法的时序图，并使用大约2×RTT的超时间隔。

（a）帧4丢失　　（b）帧4至6丢失

解答：

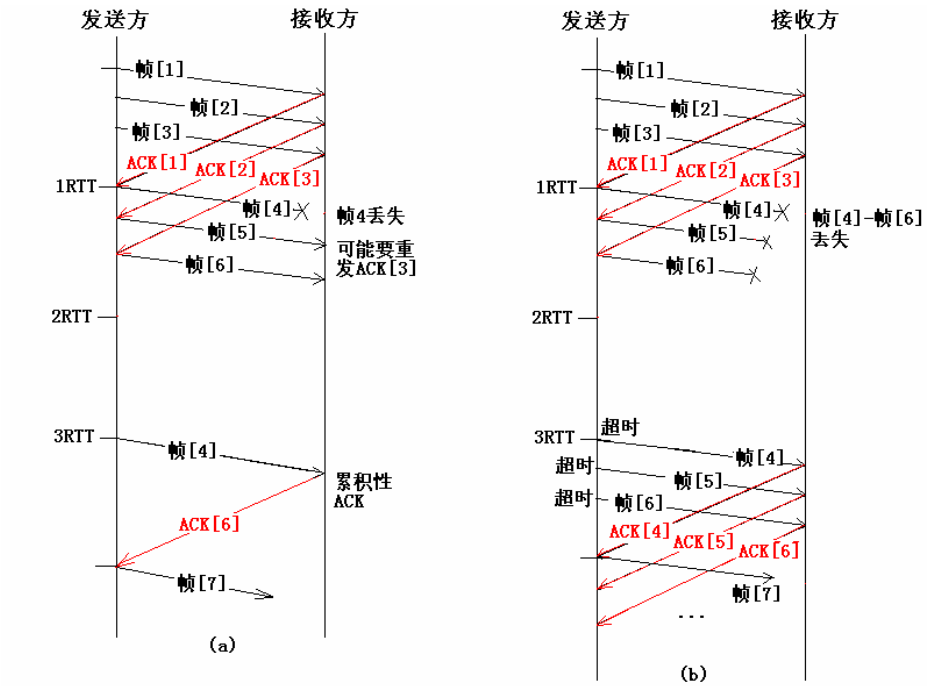


图 3-13　习题 55 插图

56. 假定我们尝试运行让SWS=RWS=3且MaxSeqNum=5的滑动窗口算法。第N个分组DATA[N]实际上包含Nmod5的序列号，即实际使用的重复出现的序列号是0，1，2，3，4，0，1，2，…。请给出一个例子，说明该算法会出现序列号混淆的问题；也就是说，在具体的操作过程中，接收方期待第5个数据分组，却接收到上次的DATA[0]，而且分不清究竟是哪一个。假定在传输过程中不会产生分组失序问题。

解答：在下列描述中，ACK[N]意味着正确地收到了所有的序列号小于（不包括等于）

N的分组。

（1）发送方发送DATA[0]，DATA[1]，DATA[2]，所有这些分组都到达了接收方。

（2）接收方发送ACK[3]，作为对0，1，2分组正确收到的应答，但这个过程很慢。接收方窗口现在是DATA[3]，DATA[4]，DATA[5]。

（3）发送方超时，重新发送DATA[0]，DATA[1]，DATA[2]。假定在重传过程中，DATA[1]和DATA[2]丢失了。接收方把重传的DATA[0]当作DATA[5]接受了，因为它们有相同的序列号0。

（4）发送方最后接收到了ACK[3]，于是现在发送DATA[3]至DATA[5]。然而接收方相信DATA[5]已经接收过了，因此把DATA[5]作为重复拷贝抛弃了。接着，协议继续正常运行，但在被接收了的流中有一个错误的分组块。

显然，如果MaxSeqNum≥6，上述问题就可以避免了。

57. 考虑SWS=RWS=3的滑动窗口算法，假定不会有帧失序现象发生，并且使用无限多个精确的序列号。

（a）说明如果DATA（6）在接收窗口中，那么就不可能有DATA[0]在来到接收方。

解答：首先我们注意到，低于发送窗口，即小于LAR（接收到的最后一个确认帧号）的帧不会再发送，而且帧在传送过程中不会发生失序现象，如果DATA[N]到达接收方，那么DATA[N-3]及序号更小的帧以后不会再到达。类似地，如果ACK[N]到达（ACK具有累积确认的效果），那么以后就不会有序号小于N的ACK到达。在本题中，我们让ACK[N]表示对所有序号小于N的数据分组的确认。

按照题意，如果DATA[6]在接收窗口中，那么窗口不会早于DATA[4]至DATA[6]，这就意味着已经发出了ACK[4]。因此DATA[1]至DATA[3]已经收到了，发送方不可能再发送DATA[0]，接收方也就不会再有DATA[0]到达。

（b）说明如果可以发送ACK[6]，那么就不可能接收到ACK[2]。

解答：如果接收方可以发送ACK[6]，那么发送方的发送窗口最低可以是DATA[3]至DATA[5]，这就意味着发送方一定已经接收到了ACK[3]。一旦接收到了一个ACK，那么以后就不可能再接收到较小的ACK，比如ACK[2]。

58. 假定如图3-14所示，A通过中间路由器R连接到B。链路A-R和R-B中的每一条每秒钟在每个方向上仅接收和发送1个分组（因此两个分组的接收和发送要花2秒钟），并且两个方向上的发送互相独立。假定A向B发送使用SWS=4的滑动窗口协议。

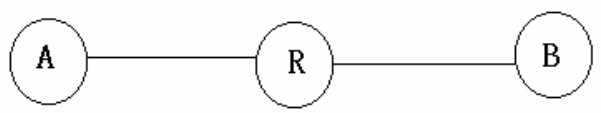


图 3-14　习题 58 插图

（a）不考虑传播延迟，对于时间T=0，1，3，4，5（秒），说明什么分组到达和离开每个接点，即给出按时序关系描述的相关事件。

解答：T=N　Data[N]离开A；

T=N+1　Data[N]到达R；
T=N+2　Data[N]到达B；ACK[N]开始返回；
T=N+3　ACK[N] 到达R；
T=N+4　ACK[N]到达A；Data [N+4]开始发送，离开A。
下面给出的是所有在行进中的分组具体的时序关系：
T=0，Data[0]至Data[3]就绪；A发送Data[0]；
T=1，Data[0]到达R；A发送Data[1]；
T=2，Data[0]到达B；ACK[0]开始返回；A发送Data[2]；
T=3　ACK[0] 到达R；A发送Data[3]；
T=4　ACK[0] 到达A；A发送Data[4]；
T=5　ACK[1] 到达A；A发送Data[5]；…

（b）如果链路具有1.0秒的传播延迟，但可以立即接受许多个分组。即延迟=1秒，但带宽无限大，那么又会发生什么样的情况？

解答：T=0 发送Data[0]至Data[3]；

T=1 Data[0]…Data[3]到达R；
T=2 数据到达B；ACK[0].. ACK[3]开始返回；
T=3 ACK到达R；
T=4 ACK到达A；A发送Data[4]…Data[7]
T=5 数据到达R。

59. 类似于上题中的图3-14，假定A通过中间路由器R连接到B。链路A-R是立即的，即带宽无限大，但链路R-B每秒钟仅发送1个分组，一次一个（因此两个分组要花2秒的时间）。假定A使用SWS=4的滑动窗口协议。试对于时间T=0，1，2，3，4秒，说明从A发往B的分组什么时候到达什么地方（包括应答分组）。

解答：T=0 A发送帧1-4；帧0开始通过链路；帧2，3，4在R的队列中。

T=1帧[1]到达B，ACK[1]开始返回；帧[2]离开R；帧3，4在R的队列中。
T=2 ACK[1]到达R，接着就到达A；A发送帧[5]到R；帧[2]到达B；B发送ACK[2]；R开始发送帧[3]；帧4，5在R的队列中。
T=3 ACK[2]到达R，接着就到达A；A发送帧[6]到R；帧[3]到达B；B发送ACK[3]；R开始发送帧[4]；帧5，6在R的队列中。
T=34ACK[3]到达R，接着就到达A；A发送帧[7]到R；帧[4]到达B；B发送ACK[4]；R开始发送帧[5]；帧6，7在R的队列中。
在R的稳态队列大小是两个帧。

60. 再次考虑习题59，其它条件不变，但假定路由器的队列长度为1，也就是说，除了正在发送的分组，它可以在队列中保持1个分组（在每个方向上都如此）。A的超时参数设

定为5秒，SWS还是4。试说明从T=0秒开始直到开头满窗口的4个分组都成功投递为止，在每秒钟的时候发生了什么样的事件。

解答：T=0 A发送帧1-4；帧[1]开始通过R-B链路；帧[2]在R的队列中；帧3和4丢失。

T=1帧[1]到达B；ACK[1]开始返回；帧[2]开始离开R。

T=2 ACK[1]到达R，接着就到达A；A发送帧[5]到R，R立即开始转发帧[5]；帧[2]到达B；B发送ACK[2]。

T=3 ACK[2]到达R，接着就到达A；A发送帧[6]到R，R立即开始转发帧[6]；帧[5]（而不是帧3）到达B；B不发送ACK。

T=4帧[6]到达B；B也不发送ACK。

T=5 A超时，重发帧3和4；R立即开始转发帧[3]；把帧[4]保持在队列中。

T=6帧[3]到达B；ACK[3]开始返回；R开始转发帧4。

T=7帧[4]到达B，并且ACK[6]开始返回；ACK[3]到达A，A开始发送帧[7]；R开始转发帧[7]。

第 4 章　局域网络和媒体访问协议

本章学习重点

- 多路访问机制
- 局域网络的体系结构
- 逻辑链路控制协议
- 令牌控制局域网
- CSMA/CD以太网
- 桥接器和局域网交换机
- 半双工和全双工以太网

4.1　基本知识点

像以太网这样的局域网络适用于诸如单个办公楼、仓库或校园这样有限的地理范围，通常跨越一个较短的距离，但以比广域网络（例如电话网、X.25网、帧中继等）高得多的速率进行数据传送。将一个网络限制在物理上较小的区域之内，比如一个楼房或一组楼房，可以减少从网络上一台计算机发送数据到最远处计算机的时延。一般说来，局域网（LAN）有3个主要特征：

（1）它们跨越一个物理上有限的距离，一般在10公里以内。
（2）以短的距离获取高数据率。
（3）它们为一个单位或组织拥有。

传统的局域网还是一个共享媒体的对等型通信网络，任一站发送的报文都以广播的形式传输，连接到共享媒体的所有其它站都可以收到报文。因此，LAN生来是不具有保密性的。连接到LAN的任何两个站都可以直接使用公共物理媒体进行点到点的通信，而不需要任何中间交换节点。另外，为了仲裁对共享媒体的使用权，在协议体系结构中总是需要有一个媒体访问控制子层。

4.1.1　多路访问机制

针对在广播媒体上的通信，有两个主要的设计方案：

- 分布式的和集中式的设计。
- 线路方式的和分组方式的设计。

在集中式设计中，网络上的一个设备担任主站的角色，它轮询每一个设备，以确定哪

个设备需要在传输媒体上发送数据。这种方法提供对媒体的非常有序的访问，但它也引入了延迟，因为即使一个设备不想通信，主站也必须依然要询问每个设备的状态。此外，如果提供轮询服务的设备失效了，那么在网络上的所有设备都不能通信。集中式系统的一个例子是蜂窝电话，每个蜂窝单元内的电话传输都要经过基站协调。

分布式设计采用分布式环境，一旦当前的通信设备停止发送数据了，需要通信的设备就可以尝试发送。但是正在等待通信并且在侦听当前会话结束的设备不知道是否有其它设备也在侦听。如果两个侦听设备同时在媒体上发送，它们的数据分组将会产生冲突。分布式设计的典型例子是以太网。

第二类设计策略关心传输媒体运载的交通类别。在网络上有两种类型的交通模式：连续的和突发的。连续的数据流意味着平滑的恒定的交通速率，例如在电话网络中的语音会话。突发性传输指网络交通突然的不可预测的增加。对于连续的交通模式，把一部分传输媒体分配给设备是有意义的，在这种情况下你不必让设备介入对媒体访问的协调过程。这种多路访问设计方法称作线路方式。

线路方式对于突发性传输工作得不好，因为突发性传输需要尽可能多的通信链路才能满足高峰时期的需求，而在通常情况下的线路利用率会很低。也就是说，如果把一部分传输媒体专门分配给每个设备，那么当一个设备不在通信的时候，分配给它的那部分媒体就会因不被使用而闲置。即使在网上因部分设备发送大量数据出现突发性交通时，这些闲置段可能因专用分配关系而仍然得不到利用。

显然我们需要为网上的设备提供一种协调对传输媒体使用的机制，采用相应的访问方法，使得能够较好地处理突发性交通。这种类型的多路访问设计方法就是分组方式。

多路访问的基本技术所要解决的主要问题是隔离来自同一通信通道上的其它设备的交通，交通隔离有时域和频域两种方法。基本技术的第二个作用是提供把时间或频率传输资源分配给在网络上的每个设备的方法。

频分（频域）多路访问（FDMA）把可提供的频率在各个设备之间划分，使得每个实体都在一个不同于其它设备的频率上发送和接收。这是一种相当简单的技术，它在模拟通信链路上工作得很好。每个频带都用警戒带隔离，因此在频率略有变化的情况下各路传输之间仍有足够的分隔。

在时分（时域）多路访问（TDMA）方法中，所有的站使用同一频率，每个设备被给予一个时槽，从而实现有序发送。这就是说，计算机A发送，然后计算机B发送，然后计算机C发送，等等。这种方法也称循环法。分配给每个设备的时间在长度上可以是固定的，也可以是可变的，并被叫做时槽。在任一时刻，一个发送设备仅可以使用一个时槽发送它的数据，然后该设备必须等待，直到它的下一个轮次才能再次发送。通过协调各个站对时槽的访问，并在所有的设备之间采用适当的时间同步，单个通信频率可以被所有的实体使用。为了取得适当的时间同步，其中有一个设备以特定的间隔时间产生同步信号。

解决多路访问问题的另一种方法是结合使用时域和频域技术。有两种可能的结合：跳频CDMA和直接序列CDMA。

在跳频CDMA（FH/CDMA）中，发送设备在一个频率上开始发送信息，然后在一段短的时间之后改变到另一个频率。这样，在一个会话期内，发送设备不断更换频率。接收设备必须使用同样的跳频图案才能正确地理解会话。在这种CDMA机制中，设备既使用时槽

技术，也使用频率技术。时槽是在一个具体的频率上使用的时间量，而频率元素则是对不同频率的使用。

直接序列CDMA（DS/CDMA）比跳频CDMA还要复杂一些，这种技术允许所有站点在整个频段上同时进行传输，多路的同时传输采用编码原理加以区分。我们可以把CDMA比喻成在一个大房间里同时进行多对的会话，不同对的人分别用不同的语言交谈，讲法语的人只理会法语，其它的就当作噪音置之不顾。在DS/CDMA中，每个比特时间被分成m个称作碎片（chip）的短的时间片。在典型的应用中，每个比特有64个或128个碎片。每个站被分配给一个具惟一性的m位代码，也称码字或碎片序列。当发送比特“1”时，它就发送它的碎片序列；当发送比特“0”时，它就发送其碎片序列的补码。只有在带宽增加到m倍的情况下，发送的信息量才能从a比特/秒增加到ma碎片/秒，这就使得CDMA成为一种扩频方式的通信。

在直接序列CDMA（DS/CDMA）中，每个站点都有自己惟一的碎片序列，所有的碎片序列都是两两正交的，也就是说任意两个不同的碎片序列S和T的内标积均为0，且任何碎片序列与自身的内标积都等于1。在每个比特时间内，站点可以发送它的碎片序列表示发送1，也可以发送其序列的反码表示发送0，还可以保持沉默什么都不干。这里假定所有的站点在时间上都是同步的，也就是说，所有的碎片序列都在同一时刻起始。要从信号中还原出单个站点的比特流，接收方必须事先知道该站点的碎片序列。通过计算所收到的碎片序列（所有站点发送的位序列的线性总和）与要还原的信息发送方站点的碎片序列的内标积，就可以还原出要得到的比特流。

4.1.2　局域网络的体系结构

传统的局域网有两个重要的特征。第一，它用带地址的帧来传送数据。第二，不存在中间交换，所以不要求路由选择。在环形局域网中使用转发器，在基带局域网中也可以使用中继器或桥接器，但它们都不含路由选择功能。局域网的这两个特征基本上确定了上述问题的答案。

虽然网络提供了物理层至网络层的3层服务，但由于局域网的特征，却允许在OSI的两个层上实现这些服务。图4-1示出了IEEE 802委员会所描述的局域网体系结构与OSI的对比。局域网的数据链路层提供的功能，与接受来自所连接站的发送信息以及交付所接收的信息给所连接的站有关。这些功能包括：

1. 提供一个或多个服务访问点（SAP）。SAP是两个相邻层之间的逻辑接口。
2. 发送时将数据组装成带有地址和差错检测段的帧。
3. 接收时拆卸帧，执行地址识别和差错检测。
4. 管理链路上的通信。

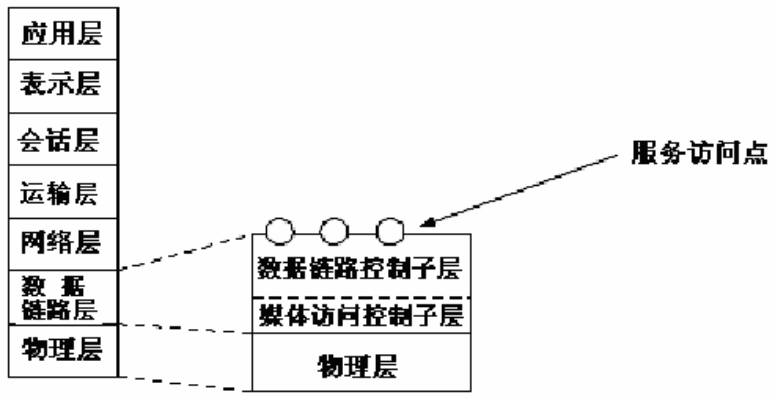


图 4-1　IEEE 802 协议层与 OSI 模型的比较

IEEE 802委员会将第1项功能定义为逻辑链路控制（LLC）子层，后3项功能则被放在另一个独立的子层，称为媒体访问控制（MAC）。之所以这样划分，一方面是在传统的数据链路控制中缺少对包含多个源和多个目的地的链路进行访问管理所需要的逻辑，另一方面在局域网上同一LLC可以有几种MAC方式的选择。

在最低一层即物理层上的功能比较明确，包括：

1. 信号的编码/译码。
2. 前导码（前缀）的生成/除去（用于同步）
3. 比特的发送/接收。

另外，802模型的物理层还包括对传输媒体和拓朴结构的说明。一般而言，这被认为是位于OSI模型最低层下面的。然而，由于传输媒体和拓朴结构的选择对LAN设计至关重要，所以也被包括在LAN协议的描述中。

4.1.3　逻辑链路控制协议

逻辑链路控制（LLC）子层用于由IEEE 802及FDDI规定的所有媒体的访问控制（MAC）标准，提供LLC用户之间通过MAC子层进行数据交换的手段。为了满足特定的可靠性及效率方面的需要，802.2规定了3种不同形式的LLC服务，即不确认的无连接服务、连接方式服务和确认的无连接服务。所有这些服务都用原语及参数进行定义。这些原语和参数在提供LLC服务的LLC实体和以LLC服务访问点（SAP）标识的LLC用户之间进行交换。

IEEE 802.2逻辑链路控制（LLC）标准与媒体访问控制（MAC）标准一起执行数据链路层的功能。LLC使用链接服务原语与网络层通信，使用媒体访问原语与MAC子层通信，并且通过传送LLC协议数据单元与通信子系统中的对等LLC实体通信。

802.2标准总的说来是基于HDLC数据链路控制协议，但又不是HDLC的帧结构。HDLC关于位填充、标志和中止序列的过程不适用于局域网，因此被LLC删除。

在使用IEEE 802.2LLC时，HDLC的地址和控制段包含在MAC帧格式数据段的开始位置。

HDLC的信息帧用于面向连接的操作，而无编号帧则用于不需要确认的无连接操作。LLC对HDLC的异步平衡方式作了若干修改，其中包括：

- 对于地址和控制段使用扩展格式（模128编号）
- 使用16位地址段存放源和目标地址，支持组目标地址
- 加入新帧UI、Test和XID
- 删除了SREJ和CMDR（FRMR-作为响应的帧拒绝）控制帧

UI用于发送用户数据，数据参数被放到UI的信息段中发往目的地。XID和TEST的使用并非由LLC用户服务请求来启动，使用这些PDU的目的在于支持管理功能，它们的信息段包含关于该PDU操作的管理信息。

4.1.4　令牌控制局域网

有多种不同类型的令牌传递网络，其中最流行的是IBM令牌环。令牌环有一个IEEE标准，称作802.5。在IBM和802.5令牌环之间有一些不同的地方。

流行的令牌环网以16Mbps的速度运行，并能用于IBM的计算机、其它生产厂商的计算机以及诸如打印机一类的外部设备。然而，FDDI（光纤分布式数据接口）标准是一种更新、更快的令牌环。事实上，FDDI是令牌环网的光纤版本。

一个令牌环网由一组连接成环的转发器构成，每个转发器经单向传输链路与另外两个转发器相连，以形成一个封闭路径，数据从一个转发器到下一个转发器逐个比特地依次传送，每个转发器重新产生并重新传输每一比特，所以称作转发器。使用转发器有两个主要目的：一是传递所有经过的帧来提供环的功能；二是为接入站发送和接收数据提供访问点（接口）。与此对应的转发器状态也有两个，即监听状态和传输状态。数据总是在一个特别的方向上绕环流动，每个节点从它的上游邻居接收帧，并向它的下游邻居转发。

环被看成是单个共享媒体，它在行为上有两个关键的特征：第一，它涉及一种分布式算法，控制每个节点什么时候被允许发送；第二，所有节点都看到网上所有的帧，在帧通过的时候，地址等于帧的头部所标识的目标地址的站保存其一个拷贝。

在令牌环中，“令牌”一词来自管理对共享环的访问的方式。其思想是让一个令牌，实际上就是一个特别的位序列，绕环旋转；每个节点都接收然后转发令牌。当一个有帧要发送的节点看到令牌时，它就把令牌从环上取下（即不转发这个特别的位序列），并取而代之地把它的帧插入环。沿途的每个节点只是简单地转发该帧，目标节点则保存一个拷贝，并把该帧继续向环上的下一节点转发。当该帧返回到发送方时，源节点把自己的帧从环上取下（不再继续转发），然后再插入令牌。这样下游的某个节点将有机会发送一个帧。实际上，当令牌绕环旋转时，每个节点都能得到发送机会。从这个意义上讲，该媒体访问算法是公平的。节点以循环轮转的方式接受服务。

跟802.5网络不同，FDDI网络由一个双环构成，两个环互相独立，一根顺时针方向传输，另一根反时针方向传输。如果有一根断了，另一根可作为后备投入使用。如果两根在同一点上都断了，例如由线槽起火或其它意外事故造成，那么两个环可以接成单一的环，，其长度约为原来的2倍。每个站都配有继电器，可以用来把两个环连接成单一的环，也可以把

出问题的某个站旁路掉。

FDDI标准规定单个网络最多可以接500个站（主机），相邻站点之间的最大距离为2公里。网络总的光纤长度限制为200公里，也就是说，由于是双环结构，连接所有站的线缆的总长度是100公里。而且，虽然在FDDI中的“F”意味着下面的物理媒体是光纤，标准也定义了可以运行FDDI的几个不同的物理媒体，其中包括同轴电缆和双绞线。

FDDI的物理层不使用曼彻斯特编码，因为100Mbps曼彻斯特编码要求200兆波特，这被认为是过于昂贵。取而代之的是5中取4编码。每组4位的MAC符号被编码成一个5位的码组。使用4比特/5比特编码方案，将4位符号转换成在媒体上传输的5位码组。

FDDI定义了两类交通：同步的和异步的。当一个节点收到令牌时，不管令牌是早到还是迟到，它总是被允许发送同步数据。与此相反，一个节点仅在令牌早到时才能够发送异步交通。

4.1.5 CSMA/CD以太网

由Xerox Palo Alto研究中心（PARC）的研究人员于20世纪70年代中期开发出来的以太网是过去20多年最流行的局域网络技术，是通用的带冲突检测的载波监听多路访问（CSMA/CD）算法在局域环境下工作的一个范例。以太网的大量使用还引发了一系列革新产品的出现，例如，快速和千兆位以太网，以及以太网交换机，它们都跟早期的以太网版本向后兼容。

1985年，IEEE为以太网制定了802.3标准。今天的以太网典型地使用双绞线或光纤作为物理介质。10BASE-T（在双绞线上的以太网）以10Mbps的速率发送数据，100BASE-T（快速以太网）以100Mbps的速率发送数据。千兆位以太网和万兆位以太网则通常运行在光纤上，并被用作企业范围的主干网络。

以太网是廉价的，它提供相对高的吞吐率和低的时延，能够支持许多应用。更重要的是，以太网为最终用户提供廉价的相对高速的网络接入途径。

以太网的介质访问控制（MAC）协议是CSMA/CD，即带冲突检测的载波监听多路访问。当使用CSMA/CD时，一个有帧要发送的节点必须等待通道空闲时才能发送。而且，该节点一边发送一边监听，一旦发现其他节点也在发送时，它就要中止发送。在中止发送之后，该节点等待一个随机长度的时间，再重复上述步骤。以太网也被说成是1持续的协议，因为每当一条忙线路变空闲时，有帧要发送的节点以1的概率发送。

发送一个遭遇冲突的帧所花的时间是一种浪费，因为参与冲突的两个节点必须中止它们的发送，并在某个随机长度的时延之后重新发送。这个浪费掉的时间跟在这两个节点之间的传播时间成正比。

在一个10BASE5或10BASE2以太网中，由于所有的计算机共享同一介质，因此传输是广播式的，冲突是可能的，并被所有的计算机检测到，CSMA/CD协议允许从所产生的帧冲突错误中恢复。

当计算机通过UTP（无屏蔽双绞线）连接到一个共同的Hub时，介质不再共享。然而，在每个端口上重发每个帧的Hub把它转变成一种广播介质。当一个Hub检测到冲突时（多于一个端口有输入信号），它发送一个阻塞信号给所有的端口，以此来仿真冲突检测机制。

当好几个Hub互连形成一个较大的网络时，由于帧在所有这些Hub的端口上重发，连接到这些Hub的所有计算机形成单个冲突域，并共享总的位速率。与此相反，桥接器和交换机有选择地重发在一个端口上接收到的帧，从而分割冲突域，使得在不同网段上的帧可以同时发送，因此增加了聚合位速率。

4.1.6　桥接器和局域网交换机

桥接器是利用全局分配的地址在串接的局域网链路之间转发帧的设备，转发决定仅仅依赖目标链路地址，这样的设备就叫做桥接器，也叫做MAC桥接器，因为它使用MAC地址。桥接器允许不涉及网络层机制的局域网的数据链路层互连。

当在任一端口上接收到一个帧的时候，桥接器检查该帧的目标地址，查表决定匹配该地址的端口。如果接收到帧的端口跟前往目的地的端口相同，那么桥接器就简单地丢弃帧；否则桥接器必须把帧在由表指定的另一个端口上转发。

早期的LAN桥接器很少有超过两个端口的。这些桥接器的性能受到当时原始的硬件和软件功能的限制，它们甚至在仅有两个端口的情况下都不能支持线性速率。这里的线性速率是指对于给定的技术，桥接器以可能的最大速率处理帧的能力。作为线速的例子，一个线速（wire-speed）10Mbps的以太网桥接器必须能够每秒钟处理14 880.9个帧，而100Mbps线速桥接器必须能够每秒处理148809个帧（平均1帧84字节）。

到了20世纪90年代，应用专有的集成电路（ASIC）、处理机和存储器技术的快速发展使得建立具有大量端口并能在所有端口上以线速转发帧的桥接器成为可能。以这种方式建立起来的桥接器被标称为交换机。应该指出，桥接器和交换机之间的差别是市场上的差别，而不是技术上的差别。交换机执行的功能跟桥接器执行的功能相同。交换机就是桥接器。市场上之所以把它们称为交换机主要是为了跟早期的比较原始的桥接器相区别。

交换LAN是传统的共享带宽LAN的替代物。以在结构化布线环境中产品的使用而言，它们之间仅有的显著差别是所使用的集线器（Hub）是交换式集线器（桥），而不是共享式集线器（重发器）。

共享式以太网LAN使用CSMA/CD MAC算法仲裁对于共享通道的使用。如果两个或更多个站同时有帧排队等待发送，在它们之间将产生冲突。我们把竞争一个共享LAN的访问的一组站称作冲突域。位于同一冲突域的站参与访问竞争，结果引起冲突和后退。位于不同冲突域的站不竞争访问一个共同信道，因此在它们之间不产生冲突。

在一个交换LAN中，每个交换机端口都是该端口的冲突域的终点。如果有一个共享LAN连接到一个指定的端口，那么，在那个端口上的所有站之间会有冲突，但在该端口上的一个站不会和交换机其它端口上的另一个站发生冲突。因此交换式集线器分隔每个端口的冲突域。

交换式集线器可以用来把传统的共享LAN分段，它也可以为网络提供集散式主干。主干网络的主要目的是互连其它网络。主干网络可以是分布式的，也可以是集散式的。在分布式主干中，主干网络面向互连的设备，地理位置分散的网络设备直接连接到主干，提供工作组级互连。在集散式主干中，主干由诸如交换机这样的高性能联网设备组成。工作组网络一般都通过点到点的链路连接到集散式主干。

当然，在另一方面，交换机也可以用来互连端点站。极端情况下，每个网段可以仅附接单个端点站，这时的网段就被称作微段。

在一个交换式集线器上，可以结合使用共享LAN连接和单个站的连接（即微段连接）。通过共享LAN连接到交换机的各个站将具有共享LAN的特征，而独占端口的站则具有微段的功能。

交换机本身是硬件设备，在外形上与路由器和网桥的差别并不大。但是，3个重要因素使交换机和其它网络设备相区别：整体速度(交换机快得多)；发送方法学或电子逻辑(更智能)；以及更多的端口数。网桥使用效率较低却较昂贵的微处理器和软件方式。交换机则更加依赖内建的逻辑板和应用专用的集成电路(ASIC)，从而操作更快且更有效。

交换机把数据流限制在局部分段，只有帧的目标主机位于其它分段时才进行跨段传输，从而提搞了速度，减少了时延。在这种情况下交换机检查目的地址，将帧仅发往目的分段，而使所有其余连至交换机的分段与此次传播无关。但是与网桥一样，交换机不阻止广播或多播。

4.1.7 半双工和全双工以太网

以太网已经从早期的同轴电缆演变为使用双绞线的结构化布线，现在双绞线是以太网采用的最普遍的物理媒体。以Hub作为星形的中心的结构化的布线系统改变了基础媒体不支持全双工操作的条件。

跟同轴电缆不同，许多种类的双绞线以太网，例如10BASE-T、100BASE-TX和100BASE-T2有可能支持双向的同时通信，因为在每个方向上的通信都有单独的双绞线通路。

当然了，即使通道能够支持双向通信，一个使用重发器Hub的以太网还只是以半双工的方式使用共享通道，因为在任一时刻仅一个网络站可以无干扰地在LAN上发送一个帧。多重发送会产生冲突，依靠通常方式的以太网媒体访问控制（MAC）予以解决。然而，采用专有的媒体至少使得以全双工方式利用通道成为可能。在LAN上采用全双工操作的条件是：

（a）只有两个网络设备连接到LAN。

（b）物理媒体本身必须能够支持无干扰地同时传输和接收。

（c）网络接口必须能够被配置成可以使用全双工方式的状态。

全双工以太网设备不使用任何MAC算法，一个站可以随意地发送，不用考虑会有其他站的干扰。全双工以太网跟半双工以太网惟一共同的方面是以太网帧格式和对物理媒体使用的编码和信号方式。

当然，支持以太网帧格式意味着提供许多重要的功能，包括地址解码以及CRC检验和的产生和验证，它们在全双工和半双工设备中都是必须的。与半双工相比，全双工操作在网络接口中并不需要附加额外的功能，只需简单地禁止半双工操作所需要的功能。这就意味着尽管在性能和应用能力方面有了增强，但全双工功能不会增加以太网接口的成本

由于全双工操作不使用CSMA/CD，这种距离限制不复成立。不管LAN的数据速率如何，全双工以太网链路的长度仅受媒体的物理传输特征的限制。尽管对于10Mbps和100Mbps的

双绞线链路能够使用的最大距离是100米，多模光纤可达2公里~3公里，单模光纤可达20公里~50公里或更长，但只要使用适当的线路驱动器和信号再生器，全双工以太网链路便可以借助卫星、专用光纤和SONET等跨越国家和国际的广域范围。

全双工操作主要用于交换机到交换机的连接，服务器和路由器的连接以及长距离的连接。

4.1.8　无线局域网

无线网络最成功的应用是蜂窝电话系统。蜂窝系统利用发射出去的信号功率随着传播距离增大而逐步衰减的事实，因此同一频道在空间上隔开一定距离的两个地段内重复使用时相互间的干扰很小。实际上，蜂窝系统把地理区域划分为邻接的不重叠的单元，让被分配给相同频道集的单元之间相隔较大的距离。每个单元有一个中心发送和接收装置（称作基站）与单元中的移动设备通信。该基站既用于控制的目的，也起一个单元中继的作用。所有的基站都跟一个移动电话交换局（MTSO）有高带宽的连接，后者又连接到公用交换电话网（PSTN）。对跨越单元边界的移动设备的移交工作通常都由MTSO处理。现代的蜂窝系统全部是数字式的，除了语音服务，这些系统还提供E-Mail、语音邮件和传呼服务等。

商业卫星通信系统是无线通信基础设施的另一个主要成分。它们在非常广大的区域提供广播服务，帮助填补在若干个高人口密度的用户区之间的覆盖间隙。卫星移动通信系统遵从跟蜂窝系统类似的基本原则，但把单元基站替换为围绕地球旋转的卫星。卫星系统典型地用卫星轨道高度、低地球轨道（LEO）、中地球轨道（MEO）或对地静止轨道（GEO:Geostationary Orbit）来表征。当前的趋势是使用较低轨道以便轻型的手持设备可以使用卫星通信。由卫星系统提供的服务包括以比较低的数据速率提供的语音、寻呼信息和消息的传送。

当用户在一个小的区域，例如一个校园或一个建筑物内，从一个地方移动到另一个地方时，无线局域网可提供高速数据传输。访问这些LAN的无线设备通常是固定的或以步行的速度移动。

所谓无线局域网（WLAN：Wireless Local Area Network）就是在互连的各主机及设备之间，不使用通信电缆或光缆等有线方式，而是采用无线通信方式。在无线网络中各节点之间的无线通信可以通过两种方式来实现。最常用的是类似于调幅或调频的无线广播系统，当然具体采用的调制技术会不同。另一种是用光来通信，类似于红外光遥控器系统。目前的无线局域网大都采用无线广播技术，最高速率可达数十兆bps。

IEEE 802.11标准制定了MAC层协议，它运行在多个物理层标准上。标准是相当复杂的。除了基本的协调访问问题，标准还结合进错误控制以克服通道固有的不可靠性，适宜的寻址和关联规程以处理站的可携带性和移动性，以及互连过程以扩展无线站的通信范围，并且允许用户在移动的同时还可以通信。

连接在无线局域网中的设备通常称作站，这些站可以是台式计算机、便携计算机，也可以是其它智能设备，例如个人数字助理、智能控制装置等。

IEEE 802.11协议使用协调功能，确定一个站什么时候被允许在无线介质上发送，以及什么时候可以在无线介质上接收PDU。为无线局域网设计的一个较早的协议是CSMA/CA，

它是IEEE 802.11无线局域网标准的基础。其基本思想就是：发送方激发接收方，使其发送一短帧，接收方周围的站点会监测到这个短帧，从而使得它们在接收方有数据帧到来期间不会发送自己的帧。

802.11工作组考虑了两种MAC 算法。一种是分布式访问控制，就像以太网那样用载波侦听的方法把介质访问的控制分布到每个站点。另一种就是集中式访问控制，由一个中央的决定者来协调对介质的访问。分布式协调功能（DCF）支持对MAC SDU做尽力而为的异步数据传送。在DCF之下，传输介质全部以竞争方式运行，所有的站需要为每个要发送的分组竞争通道。IEEE 802.11还定义了可选的点协调功能（PCF），它可以通过一个AP实现，支持对MAC SDU做面向连接的时限传输。在PCF之下，介质可以在竞争期（在此期间介质使用竞争方式）和无竞争期（CFP）之间交替。在无竞争期内对介质的使用由AP控制，因而免除了站竞争通道访问的需求。分布式访问控制对于那些有突发通信量的无线网是有吸引力的。集中式控制适用于几个无线站点的互连以及跟有线主干网的连接，对于时间敏感的或拥有高优先级数据处理的应用就更重要了。

除了802.11局域网，还有LMDS（本地多点分布业务）无线本地回路，它可以复盖社区的局部范围(3—6km)，支持双向的广播视频、视频点播、数据和电话业务，使用27.5—28.35GHz、29.10—29.25GHz和31.00—31.30GHz范围内的频率，总共可得到1.3GHz的带宽。其缺点是在这样高的频率上无线电波的波长很短，容易衰减，因此许多LMDS系统采用数字中继器来扩大接入网的地域。它们的采用受同波道干扰范围的制约。为了解决这个问题，一些经营者转向扩展频谱和码分多址(CDMA)，以求相邻的地域单元可以共享同一个频谱空间。基于LMDS，IEEE 制定了802.16宽带无线网络标准。

在短距离无线通信方面，蓝牙技术试图使用廉价的低功耗无线电互连计算、通信设备和部件。虽然最初的想法是免除设备之间的线缆，但很快就扩展到无线局域网的范围。1999年，蓝芽 SIG（特别兴趣组）发布了1500页的技术规范V1.0。过后不久，IEEE以蓝牙的这个版本为基础制定了无线个人区域网（PAN）标准802.15。值得注意的是，蓝牙规范包括整个系统，从物理层到应用层；而802.15标准只涉及物理层和数据链路层。

4.2 基本练习题

1．什么是局域网？

解答：局域网（LAN）是指一组计算机及其它设备分布在一个有限的地理区域内，并且彼此间通过通信网络相互连接。通常LAN局限于一个建筑物或一个园区内。

2. 标准10Mbps 802.3局域网的波特率是多少？

解答：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10Mbps，因此波特率是数据率的两倍，即20M波特。

3. 一个局域网可以有路由器吗？

解答：可以。局域网通常包含多个路由器，把局域网划分成多个较小的广播域。局域网这个术语描述地理布局，而不是OSI模型第2层和第3层之间的区别。

4. 在比较流行的术语中，分组和帧之间的差别是什么？

解答：在比较流行的术语中，帧是数据链路层PDU，而分组是网络层PDU。换句话说，在分组上加数据链路层头和尾形成帧。因此帧是封装分组产生的。

5. 填空题

IEEE的局域网模型包括三个层次（含子层），它们分别是_____层、_____子层和_____子层。为了表示所有可能的高层协议，Internet团体对IEEE 802.2 LLC头部做了扩展，定义了_____协议。该标准将通用SAP段的值置成_____，是要告诉目的地LLC层查看帧中数据段开头5个字节，在那里有关于厂商或团体和高层协议的说明。

解答：IEEE的局域网模型包括三个层次（含子层），它们分别是物理层、逻辑链路控制子层和媒体访问控制子层。为了表示所有可能的高层协议，Internet团体对IEEE 802.2 LLC头部做了扩展，定义了子网访问协议。该标准将通用SAP段的值置成AA，是要告诉目的地LLC层查看帧中数据段开头5个字节，在那里有关于厂商或团体和高层协议的说明。

6. 帧是如何被路由通过网络的？

解答：帧不会被路由通过网络。一个帧仅存在于一个广播域内。如果在帧内的分组前往一个远方的网络，路由器会把分组拷贝到它的缓冲区，然后丢弃帧。一旦路由器确定了外出接口，它就建立一个新帧，把分组放到新帧内，并把分组继续向前发送。

7. 环网是如何控制媒体访问的？

解答：大多数环网使用令牌传递的方法。令牌是一个特别的帧，从一台计算机发送到在环方向上的下一个最近的邻居。该邻居再把令牌传送到在环上的下一个设备，等等。仅仅拥有令牌的设备被允许访问媒体。换句话说，如果你要发送一些数据，你必须等待你的上游邻居给你发送令牌，在得到令牌后再发送你的数据。在你发送数据之后，你把令牌传递给下一个计算机，使得它也有发送的机会。

8. 任意网状的网络是怎样控制媒体访问的？

解答：实际上，任意网状的网络典型地是不控制媒体访问。因为在每条链路上仅有两个设备，而且连接一般都是全双工的，这就意味着两个设备可以同时说和听，没有必要控制媒体访问。

9. 判断题

令牌环网络可能有冲突。

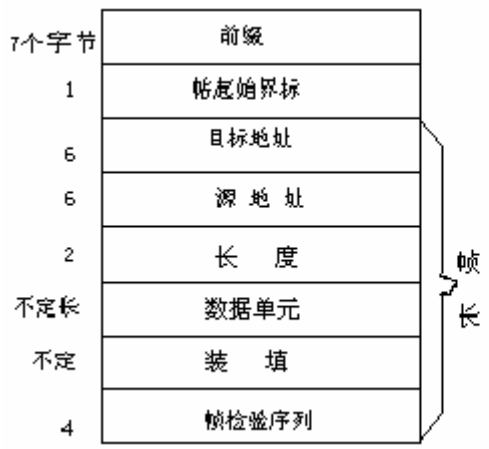
a．真　　b. 伪

解答：b. 伪。在令牌环网络上不可能有冲突。

10. 令牌环的差分曼彻斯特编码跟以太网的常规曼彻斯特编码有什么不同？

解答：常规曼彻斯特编码使用从高电压到低电压的跳变表示1，从低电压到高电压的跳变表示0。而差分曼彻斯特编码用位时间的起始边界是否存在一个跳变分别表示0和1。

11．图4-2示出了在一个IEEE 802.3 标准以太网（10BASE5）上使用的帧格式，请参照这一格式完成下列关于局域网的问题填空。



（1）前缀由二进制的_____位序列重复七次组成，帧起始界标则是固定的二进制位序列_____。

（2）如 果帧长按图中所示范围计算，那么允许的最小帧长是_____字节，允许的最大帧长等于_____字节。

（3）如果一个帧的数据单元段长度是40字节，那么该帧中装填段的长度 应该是_____字节。

图 4-2　习题 10 插图

解答：

（1）前缀由二进制的__10101010__位序列重复七次组成，帧起始界标则是固定的二进制位序列__10101011__。

（2）如 果帧长按图中所示范围计算，那么允许的最小帧长是__64__字节，允许的最大帧长等于__1518__字节。

（3）如果一个帧的数据单元段长度是40字节，那么该帧中装填段的长度 应该是__6__字节。

12. IEEE 802.2定义了三种LLC协议或称操作模式，其中，

类型1操作支持_____服务
类型2操作支持_____服务
类型3操作支持_____服务

解答：

类型1操作支持___不确认的无连接____服务

类型2操作支持_____连接方式_____服务
类型3操作支持____确认的无连接____服务。

13. （选择题）术语“有效容量（goodput）”用来定义传输的下列特征：

（a）传输链路运载重传分组的那部分容量
（b）在传输链路上传输的非重传的那些分组
（c）传输链路运载非重传分组的那部分容量

解答：.c. 传输链路运载非重传分组的那部分容量。如果在媒体上没有由于拥塞或其它因素引起的分组丢失，理想环境的有效容量将等于1.0。

14. 说明轮询（polling）和探查（probing）之间的差别。

解答：在轮询方法中，主站询问每个站是否有数据要发送。如果被询问的站有数据要发送，它就直接发给接收站；或者发到主站，再由主站转发给接收站。如果被询问的站没有数据要发送，主站继续询问下一个设备。轮次询问每个站，直到所有的设备都被询问。然后主站再轮流询问每个设备。轮询系统的一个缺点是一个有数据要发送的站在得到发送许可之前需要等待较长的时间。在这个要发送的站之前，主站需要询问在线的所有其它设备。例如，即使一个设备有多个分组要发送，而所有其它的站都没有数据要发送，该单个活动站在它要发送的每个分组之间也必须等待所有其它设备被主站询问。

探查是轮询的一个变种，它给每个设备分配一个连续的地址。在线的每个设备依次得到在媒体上传输的机会。该方法要比标准轮询方法好一些，因为主设备不用介入每次传输。当然，每个设备必须能够接收发送给它的地址的信息以及作为广播或多播发送给它所在的组的报文。作为例子，考虑在利用卫星转发的数据传输的情况下，让卫星轮询每个地面站的方案是不可取的，因为每个“轮询/响应”都需要270毫秒的时间。然而，如果所有的地面站都连到一个（典型的是低带宽的）分组交换网络，使用探查方法是可能的。其思想是把所有的站都安排进一个逻辑环中，因此每个站都知道它的前驱。在这个地面环中循环转动一个令牌，但卫星看不到这个令牌。仅当捕获到令牌时，一个站才能在上行链路上发送。如果站的数目少且相对恒定，那么令牌传输时间是短的。在上行通道中发送的突发交通量则要比令牌旋转时间长得多。因此，采用该访问机制是适度的和有效的。

15. 解释在基于预留的媒体访问机制中使用小槽代替常规的数据槽的理由。

解答：在像是卫星传输这样的快速、长延迟的网络上，轮询和线路方式交换技术是不可行的。在这种情况下，基于预留的访问机制是一个好的解决方案。在基于预留的系统中使用两种类型的时槽。一种类型运载由有数据要发送的设备产生的预留报文。另一种类型的时槽用以运载数据，因为预留时槽比数据时槽小，所以也叫做小槽。

当使用较小的时槽处理预留请求和其它管理任务时，在小槽上发生的冲突对数据传输没有多大的影响。

16. 试述在p持续CSMA和非持续CSMA之间的差别。

解答：CSMA（载波感应多路访问）方法结合使用了一种各个设备可以使用的检测媒

体是否正在被使用的机制。如果一个要发送的站“听到”在媒体上有分组在传送，该站在可以发送之前必须等待。采用CSMA，需要一种算法来决定，当发现媒体忙时如何处理。常用的有三种算法。第一个载波侦听协议叫做1-持续CSMA。当一个站点要传送数据时，它首先侦听信道，看是否有其它站点正在传送。如果信道正忙，它就持续等待，直到当它侦听到信道空闲时，就立即将数据送出。若发生冲突，站点就等待一个随机长的时间，然后重新开始侦听信道，此协议就叫做1-持续CSMA，因为站点一旦发现信道空闲，其发送数据的概率是1。第二个载波侦听协议是非持续CSMA（non-persistent CSMA）。在该协议中，站点比较“理智”，不像第一种协议那样“贪婪”。在发送之前，站点会侦听信道的状态。如果没有其它站点在发送，它就开始发送。但如果信道正在使用之中，该站点将不再继续侦听信道，而是等待一个随机的时间后，再重复上述过程。凭直觉，这种协议会比1-持续CSMA协议的信道利用率高，但时延可能会长些。最后一个协议是P-持续CSMA（P-persistent CSMA），它用于分隙信道，其工作过程如下：一个站点在发送之前，首先侦听信道，如果信道空闲，便以概率P传送，而以概率q=1-p把该次发送推迟到下一时隙。如果下一时隙仍然空闲，便再次以概率p传送而以概率q把该次发送推迟到下下个时隙。此过程一直重复，直到发送成功或者另外一站开始发送为止。在后一种情况下，该站的动作与发生冲突时一样（即等待一随机时间后重新开始）。若站点一开始就侦听到信道忙，它就等到下一时隙，然后重新开始上述过程。

17. 二进制指数后退的含义是什么？

解答：在二进制指数后退算法中，如果一个发送设备检测到了一次冲突，它就后退，等待一个随机的时间长度。推迟的时间必须是时隙（slot time）的整数倍。时隙是冲突处理的时间单位，它大于物理层往返传输时间，其值跟网络的具体实现有关，比如在基带类型10BASE5中该值是512位。延长多少时隙选为均匀分布的随机参数r，$0 \le r \le 2^k$，其中k=min(n,10)，n为重发次数。用来产生随机值r的算法应使任何两个站产生相关值的可能性最小。每当该站在重发数据之后又检测到冲突时，都要把后退的时间长度加倍。对这种延迟时间加倍的实现产生了按指数后退的定时器。

18. （选择题）在以太网上“阻塞（JAM）”信号的功能是什么？

（a）当发现冲突时，CSMA/CA发送一个“阻塞”信号。当所有的站都检测到阻塞信号时，它们立即停止发送尝试。

（b）当发现冲突时，CSMA/CD发送一个“阻塞”信号。当所有的站都检测到阻塞信号时，它们立即停止发送尝试。

（c）当媒体空闲时，CSMA/CD发送一个“阻塞”信号。当所有的站都检测到阻塞信号时，它们立即开始竞争访问媒体。

（d）当媒体空闲时，CSMA/CA发送一个“阻塞”信号。当所有的站都检测到阻塞信号时，它们立即开始竞争访问媒体。

解答：b。当发现冲突时，CSMA/CD发送一个“阻塞”信号。当所有的站都检测到阻塞信号时，它们立即停止发送尝试。然后，该设备在再次尝试发送之前使用一个二进制指数后退例行程序等待一个时间间隔。

19. 在一个CSMA/CA网络上，计算机A有一个2时槽的帧间间隔，计算机B的帧间间隔是6时槽，计算机C的帧间间隔是4时槽。哪个设备具有最高的优先级？

（a）计算机A　　b. 计算机B　　c. 计算机C

（b）在CSMA/CA网络中不能够分配优先级

解答：a. 计算机A。 CSMA/CA基本上是一种p持续机制，加上空闲时间管理。当一个设备检测到传输媒体空闲时，该设备在它可以竞争访问媒体之前必须等待一个指定的帧间间隔（IFS）时间。帧间间隔也可以用于优先级传输。如果一个设备被分配一个较小的帧间间隔值，那么它就有更多的机会得到对传输媒体的访问。在本题的3个设备中，　　计　算机A具有最小的帧间间隔值，因此具有最高的优先级。

20. 什么是暴露终端问题？

解答：控制无线媒体访问的最简单元的方法是使用CSMA（载波侦听多路访问），侦听是否有其它发送者，如果没有，自己就可以发送。但实际上该协议是行不通的，因为虽然在发送方不会互相干扰，但在接收方会产生干扰。为了把这个问题解释清楚，考虑图4-3中所示的情况。

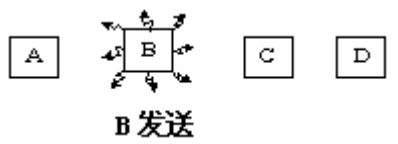


图 4-3　习题 20 插图

图中画出了4个无线站点。其中A和B的无线电波范围互相重合并且可能互相干扰。C可能干扰B和D但不会干扰A。现在假定B向A发送，C在侦听，它会听到正在进行的发送并且错误地认为不能向D发送，但实际上它的发送只会在B和C之间的区域产生错误的接收，D是可以得到正确的接收的。这种情况有时被称为暴露终端问题。关键的问题是，在开始传送之前基站真正想知道的是在接收方周围是否还有其它传送活动。而CSMA却只告诉在要发送的站点自己周围是否有传送活动在进行。在有线方式下，所有的信号会传播到所有的站点，因此在同一时刻只能产生一个发送。但在基于小范围无线电的系统中如果多个发送者的目标均不相同并且传送范围互不影响，那么就可同时进行。为了解决这个问题，人们设计了一种称作BTMA（忙音多路访问）的机制。BTMA把可用的频带划分成数据（报文）通道和忙音通道。当一个设备在接收信息时，它把数据既一个“音”放到忙音通道上。其它要给该接收站发送数据的设备在它的忙音通道上听到忙音，知道不要发送数据。假定有3台计算机，计算机B可以听到计算机A和计算机C，但计算机A和计算机C 互相听不见。使用BTMA，计算机A就可以知道计算机C在发送，因为计算机A可以在计算机B的忙音通道上接收到由于C的发送而引起的忙音。在暴露终端的情况下，在一个单元中的一个设备检测不到在邻接单元的忙音通道上的忙音。

21. 选择题

在BTMA（忙音多路访问）机制中，忙音的目的是什么？

（a）当其它设备在一个设备的忙音通道上没有听到忙音时，它们知道不要发送数据，因为媒体正在被使用。

（b）网络上现在没有在发送的设备发出一个忙音，使得其它设备知道媒体是空闲的。

（c）网络上现在没有在发送的设备发出一个忙音，使得其它设备知道媒体不是空闲的。

（d）当其它设备在一个设备的忙音通道上听到忙音时，它们知道不要发送数据，因为媒体正在被使用。

解答：d. 当其它设备在一个设备的忙音通道上听到忙音时，它们知道不要发送数据，因为媒体正在被使用。

BTMA把可用的频带划分成数据（报文）通道和忙音通道。当一个设备在接收信息时，它把数据既一个“音”放到忙音通道上。其它要给该接收站发送数据的设备在它的忙音通道上听到忙音，知道不要发送数据。这种机制帮助减少隐藏终端和暴露终端的问题。假定有3台计算机，计算机B可以听到计算机A和计算机C，但计算机A和计算机C 互相听不见。使用BTMA，计算机A就可以知道计算机C在发送，因为计算机A可以在计算机B的忙音通道上接收到由于C的发送而引起的忙音。在暴露终端的情况下，在一个单元中的一个设备检测不到在邻接单元的忙音通道上的忙音。

22. 在一个令牌环网络上，当令牌被破坏了的时候将会发生什么样的后果？

解答：如果令牌被破坏了，令牌环网络将停止服务，因为各个站都没有令牌可用。为了帮助减少这一故障的影响，网络指定一个设备起一个监控器的作用。它在令牌被破坏或丢失时将产生一个新的令牌。

23. 选择题

当在同一局域网上的两个设备具有相同的静态MAC地址时会发生什么样的情况？

（a）首次引导的设备排它地使用该地址，第二个设备不能通信

（b）最后引导的设备排它地使用该地址，另一个设备不能通信

（c）在网络上的这两个设备都不能正确通信

（d）两个设备都可以通信，因为它们可以读分组的整个内容，知道哪些分组是发给它们的，而不是发给其它站的。

解答：c. 在网络上的这两个设备都不能正确通信。在使用静态地址的系统上，如果有重复的硬件地址，那么这两个设备都不能通信。在局域网上的每个设备必须有一个唯一的硬件地址。

24. 选择题

什么是FDD（Frequency Division Duplex: 频分全双工）？

（a）FDD是一种允许专用通信的频分技术。

（b）FDD是一种允许动态媒体分配的频分技术。

（c）FDD是一种允许有保证的信息投递的频分技术。

（d）FDD是一种允许双向或全双工通信的频分技术。

解答：d. FDD是一种允许双向或全双工通信的频分技术。两个通信设备使用不同的频率获得全双工的会话。

25. 给出一种方法，你可以用来免除局域网多路访问的问题。

解答：在局域网上免除局域网多路访问问题的一种方法是通过使用点到点的通信链路。在这种类型的连接方案中，对于传输没有竞争，因为每条链路仅有两个设备。

26. 什么是隐藏终端问题？

解答：控制无线媒体访问的最简单元的方法是使用CSMA（载波侦听多路访问），侦听是否有其它发送者，如果没有，自己就可以发送。但实际上该协议是行不通的，因为虽然发送方不会互相干扰，但在接收方会产生干扰。为了把这个问题解释清楚，图4-4所示的情况。图中画出了4个无线站点。其中A和B的无线电波范围互相重合并且可能互相干扰。C可能干扰B和D但不会干扰A。

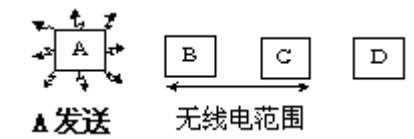


图 4-4　习题 26 插图

现在假定A向B发送，C在侦听，因为A在C的范围之外，所以C听不到A，它会错误地认为它也可以发送。如果C确实也在此时开始发送，它就会干扰B，从而破坏了从A传来的帧。由于可能的竞争者相离太远，导致基站不能监测到的问题有时被称作隐藏终端问题。关键的问题是，在开始传送之前基站真正想知道的是在接收方周围是否还有其它传送活动。而CSMA却只告诉在要发送的站点自己周围是否有传送活动在进行。在有线方式下，所有的信号会传播到所有的站点，因此在同一时刻只能产生一个发送。但在基于小范围无线电的系统中如果多个发送者的目标均不相同并且传送范围互不影响，那么就可同时进行。

换一个角度看待这个问题，假设办公大楼内所有的雇员都有一台无线便携式计算机。现在李明想给王华发送一条消息。李明的计算机会侦听其周围的环境，如果没有其它发送活动，就开始发送。但是在王华的办分室内仍有可能会产生冲突，因为也许有第三者正在向王华发送消息，但他的位置离李明太远，李明的计算机不能监测到他的活动。

为了解决这个问题，人们为无线局域网设计了称作“避免冲突的多路访问（MACA——Multiple Access With Collision Avoidance）”的协议。它被采用为IEEE802.11无线局域网标准的基础。其基本思想就是：发送方激发接收方，使其发送一短帧，因此接收方周围的站点就会监测到这个短帧，从而使得它们在接收方有数据帧到来期间不会发送自己的帧。

4.3　综合应用练习题

1．　一组N个站点共享一个56kbps的纯ALOHA信道。每个站点平均每100秒输出一个

1000比特的帧，即使前一个帧还没有发送完也依旧进行（例如，站点都有缓存）。N的最大值是多少？

解答：对于纯ALOHA，可用的带宽是0.184×56kbps=10.304bps

每个站需要的带宽是1000÷100=10bps

因此N=10304÷10≈1030

所以，最多可以有1030个站，即N的最大值是1030。

2. 如果一个以太网适配卡经历5次连续冲突，那么它将等待多少个位时？

解答：使用公式　$0<r<2^k$

在这里 k=min(n,10)

现在n=5，因为5 <10,所以k=5,2^k=32.

因此，将要等待的时隙（ slot time）的个数的随机值应从0至32的范围内选取。时隙是冲突处理的时间单位，它大于物理层往返传输时间。在基带类型10BASE5中该值被标准化为512个位时。如果随后又有更多的冲突发生，选取范围将呈指数型增长，极限值是从0到1024的范围内随机选择等待的时隙数目。

3. 广播子网的一个缺点是有多个主机试图访问信道时造成的信道容量浪费。作为一个简单例子，假设把时间分为离散的时间片，n台主机中每一台主机在每个时间片内试图占有信道的概率为p。求由于冲突被浪费的时间片的比例。

解答：先区别n+2种事件。从事件1直到事件n都是由对应的主机试图使用通道而不发生碰撞获得成功的条件形成。这些事件中的每一个的概率都$p（1-p）^{n-1}$。事件n+1是一个空闲通道，其概率是$（1-p）^n$。事件n+2是一次碰撞。由于这n+2个事件是穷举的和完备的，它们概率的和必定是1。因此，碰撞的概率，即浪费的时间片的比率是：

$1-np（1-p）^{n-1}-（1-p）^n$

4. 多路访问机制的4个性能参数是什么？

解答：（1）正常吞吐率或有效带宽（goodput）

它是传输链路运载非重传分组的那部分容量。由协议引入的开销、分组冲突和重传所花的时间不计入goodput的性能值。如果在媒体上没有由于拥塞或其它因素产生的分组丢失，那么理想环境的goodput值将等于1。在今天的网络上使用的大多数协议和系统都具有在1和0.95之间的goodput值。

（2）平均延迟

它等于分组在发送方可以被发送之前等待的平均时间加上发送该分组所化的时间。影响该参数的因素包括发送设备的工作负荷，以及传输媒体的特征。

（3）稳定性

它是多路访问机制控制交通量的增加而又不影响吞吐率的能力。当越来越多的设备在传输媒体上通信的时候，冲突的机会增加；当达到一个门槛值时系统变得不可用，并且不再稳定。如果多路访问技术包括调节的能力，以适应到达过载的条件，那么该技术就能成

功地处理交通的增加。

（4）公平性

它的含义是再一个指定的帧时内要发送的每个设备对媒体都有平等的访问权力。

5. 对比纯ALOHA和分槽ALOHA在低负载条件下的延迟，哪一个比较小？请说出原因。

解答：对于纯ALOHA，发送可以立即开始。对于分槽ALOHA，它必须等待下一个时槽。平均地讲，这要引入半个时槽的延迟。因此，纯ALOHA的延迟比较小。

6. 在多路访问的设计中，参数a表示在离得最远的设备可以收到任何数据位之前发送设备可能放到通信媒体上的分组的个数或者一个分组的几分之几。参数a可以定义成：

a=D/T

这里的D表示以秒计的最大传播延迟，T是一个平均大小的分组以秒计的传输时间。

如果在一个网络中，平均分组大小是400字节，带宽是10Mbps，传播延迟是120微妙，一个分组的传输时间是12微妙。那么该网络的a参数是多少？

解答：a=D/T

D是以秒计的最大传播延迟，T是一个平均大小的分组以秒计的传输时间。现在传播延迟时120微妙，一个分组的传输时间是12微妙，即D=120微妙，T=12微妙，所以，

A=120/12=10

7. 一万个航空定票站在竞争使用单个分槽ALOHA通道。各站平均每小时做18次请求。一个槽是125微妙。总的通道负载约为多少？

解答：每个终端每200（=3600/18=200）秒做一次请求，总共有10000个终端，因此，总负载是200秒做10000次请求，平均每秒50次请求。每秒8000个时槽，所以平均每个时槽发送次数是G=50÷8000=1/160.

8. 在FDDI网络中，反向旋转双环的含义是什么？

解答：反向旋转双环是两个平行的物理环，数据在每个环上沿相反方向传输。为了完成这种配置，每个设备必须有两个发送器和两个接收器，因此它可以在两个环上通信。

9. 在传输媒体出现故障时，反向旋转双环可以怎样帮助从故障中恢复？

解答：在反向旋转双环的大多数实现中，两个环中仅一个环（主环）用于数据传递，另一个环用于管理和作为在主环发生故障时的备份。当环上有一个断点或有一个设备发生故障时，在两个环之间形成一个链接，使得数据可以绕过故障点进入次环，然后再回到主环，从而使数据传输得以继续进行。

10. 对一无限用户分槽ALOHA信道的测量表明10%的时槽是空闲的。

（a）信道载荷G是多少？

（b）吞吐率是多少？

（c）信道是过载还是载荷不足？

解答：（a）从泊松定律得到$p_0=e^{-G}$

因此$G=-\ln p_0=-\ln 0.1=2.3$

（b）$S=Ge^{-G}$，$G=2.3$，$e^{-G}=0.1$

$S=2.3\times 0.1=0.23$

（c）因为每当G>1时，信道总是过载的，因此在这里信道是过载的。

11. 为什么跳频CDMA（FH/CDMA）机制既需要考虑频率，又需要考虑时间？

解答：跳频CDMA多路访问方法结合了时域和频域技术。在跳频CDMA中，发送设备在一个频率上开始发送信息，然后在一段短的时间之后改变到另一个频率。这样，在一个会话期内，发送设备不断更换频率。接收设备必须使用同样的跳频图案才能正确地理解会话。在这种CDMA机制中，设备既使用时槽技术，也使用频率技术。时槽是在一个具体的频率上使用的时间量，而频率元素则是对不同频率的使用。

12. 为什么要开发CSMA/CA？

解答：在一些网络（例如无线局域网）上，系统不能够检测冲突，因为发送设备的功率要比接收设备的功率强得多。在这种情况下，冲突检测是不可行的，设计一个能够帮助避免冲突的系统更有意义。因此人们开发了带避免冲突的CSMA，即CSMA/CA。

13. 请求发送的帧随机地到达一个100Mbps的通道。当一个帧到达时，如果通道忙，它就在队列中等待。帧的长度呈指数分布，平均每帧10，000位。针对下列每一种帧到达速率，给出一个平均帧所经历的延迟，包括排队时间和发送时间。

解答：本题需要使用Markov排队理论的标准公式

$$T=\frac{1}{\mu c-\lambda}$$

T表示一个容量c比特/秒的通道的平均时延，到达速率为λ帧/秒，每个帧的长度是指数概率密度函数，平均每个帧$1/\mu$ 位。服务速率是每秒μc个帧。在本题中，$c=10^8$, $\mu=10^{-4}$, 因此

$T=1/(10000-\lambda)$

（a）90帧/秒

$T=1/(10000-90)=0.1\times 10^{-3}$秒=0.1毫秒

（b）900帧/秒

$T=1/(10000-900)=0.11\times 10^{-3}$秒=0.11毫秒

（c）9000帧/秒

$T=1/(10000-9000)=1\times 10^{-3}$秒=1毫秒

14. 试述分槽ALOHA（S-ALOHA）和预留ALOHA（R-ALOHA）之间的差别。

解答：在分槽ALOHA中，环境的时基（time base）被划分成同样间隔的时槽。当一个站有数据要发送时，要等到下一个时槽开始时才能开始发送。这个策略的效果是把ALOHA

冲突窗口的大小减半，从而把有效吞吐率加倍，达到大约36%。分槽ALOHA的代价是需要有一个时间同步系统。

在预留ALOHA中，时间被划分成时槽，每个设备被分配一个时槽，专门为该设备排它使用而预留。时基被划分成由固定个数的时槽组成的帧。当一个设备使用预留ALOHA得到对一个时槽的访问时，它也就得到了该时槽所来自的帧的随后的所有时槽。该机制也可以帮助减少冲突，因为一个设备一旦得到一个时槽，那么在该帧的剩余时槽中其它设备不会发送。值得注意的是，预留ALOHA中没有主站，每个站都检查预留请求，并确定哪个站拥有哪个预留槽。预留ALOHA不支持优先级。

15. 在一个LAN上使用下列协议，在最坏的情况下一个站s在可以开始发送它的帧之前必须等待多长时间？

（a）基本的位图协议

解答：它的竞争周期恰好由N个时槽组成（假定有N个站，每个站都有一个唯一的地址，从0到N-1）。如果站0想发送一帧，它就在第0个时槽内发送比特1。在该时槽内不允许其它任何站发送。无论站0干了什么，只要站1有1帧在排队等待发送，它就可以在第1个时槽内发送比特1。一般地，站j可以通过在时槽j内填入比特1来声明它有一帧要发送。在N个时槽过后，每个站都知道究竟有哪些站要发送，然后它们就按照序号从小到大的顺序依次发送。

最坏的情况是：所有的站都要发送，并且s是最低序号站。s站要等待其它N-1个站都发送完一帧，并且再等待N位竞争期，才可以发送自己的帧。这样总的等待时间等于

N+(N-1)d位时，其中d是每个数据时槽内可发送的位数。

（b）变更虚拟站号的Mok和Ward协议

解答：在采用二进制倒计数法的协议中，每个要使用信道的站首先将其地址以二进制位串的形式，按照由高到低的顺序进行广播，并且假定所有地址的长度相同。然后各站的地址的对应位进行布尔或运算。如果某站发现其地址中原本为0的高位被置换为1，那么它便放弃发送。在总共有 你个站的情况下，地址长度为$\log_2 N$。该方法的信道效率为$d/(d+\log_2 N)$，其中d是每个数据时槽内可发送的位数。

Mok和Ward提出的协议是二进制倒计数法的一个变种。该协议使用虚拟站号，每次传输之后，对站重新编号，从0开始，已经成功传送了一帧的站排在最后。这样，长时间沉默的站会获得较高的优先权。

最坏的情况是，所有的站都有帧要发送，并且s具有最低的序列号。S站要等待其它N-1个站都发送完一帧，并且再等待N个竞争期（每个长度都是$\log_2 N$），才可以发送自己的帧。这样总的等待时间等于（N-1）$d + N\log_2 N$位。

16. 在什么情况下应把你的设计从忙音多路访问（BTMA）改变成带冲突避免的多路访问（MACA）？

解答：忙音多路访问需要细分频率，这可能在数据和忙音通道之间引入串音或干扰的机会。如果发生了串音，那么一个站在没有任何数据时可能检测到忙音，或者在没有任何数据时可能检测到忙音，或者一个设备在没有相关的忙音的情况下检测到数据。因此它不

能确定谁在使用媒体。在MACA中也使用忙音概念，但忙音是在数据通道上作为特殊的报文发送，使得所有的站都知道接收方处于忙状态，媒体正在被使用。显然在把频率细分成数据通道和忙音通道会引入串音的情况下应把设计方案从BTMA改成MACA。

17. 无线局域网使用MACA(带碰撞检测机制的多路访问)一类的协议，而不是CSMA/CD。那么，在什么样的条件下可以使用CSMA/CD来替代MACA呢？

解答：无线局域网不能采用以太网的CSMA/CD,其原因有三个方面。第一，在无线环境中检测冲突是困难的，因此不可能中止互相冲突的传输。第二，无线环境不像有线广播媒体那样好控制，来自其它LAN中的用户传输会干扰CSMA/CD的操作。第三，无线LAN存在隐藏站点问题。

具体地讲，CSMA/CD可以使用同样的信号频率同时发送和接收，但无线不能够在同一频率上发送和接收。即使这个问题可以解决（例如每个站有两个无线装置），还有另一个问题，并非所有的站互相都在有效的无线范围之内。如果所有站的发射有效范围都很大，以致于任一站都可以收到所有其它站发送的信号，那么任一站都可以跟其它站以广播方式通信。只有解决了这两个问题，CSMA/CD才能成为无线局域网协议的竞争者。

18. 给设备分配硬件地址可以用三种不同的方法：静态的，可配置的，或动态的。对于这些方法中的每一种，说明在网络上出现重复硬件地址时，可能是什么原因或哪个设备的错误引起这样的故障。

解答：如果是在使用静态地址的系统上发生重复硬件地址问题，那么错误是由设备制造厂商造成的。管理员不能够改变地址。在地址可配置的环境中，错误是由管理员造成的，是他负责把当前在使用的地址存档。在动态分配地址的环境中，重复地址可能由多种原因引起。例如，如果传输媒体有问题，那么检查一个地址是否已被使用的设施可能接收到不正确的信息。在另一方面，如果建在该设施内部的确定硬件地址是否重复的例行程序设计得不正确，那么故障的责任就在厂商那里。

19. 六个站（A、B、C、D、E和F）使用MACA协议通信。有可能两个发送在同时进行吗？请解释你的回答。

解答：有可能。假定它们在一条直线上，每个站仅能够到达最近的邻居。那么，在A给B发送的同时，E可以在给F发送。

20. 假定有一个10Mbps的网络，其平均分组长度是110字节，峰值吞吐率是每秒9500个分组，试计算该网络的正常吞吐率（goodput）？

解答：在一个平均分组长度是110字节、峰值吞吐率是每秒9500个分组的10Mbps的网络上，承载容量是每秒11 364个分组（$=10\times10^6\div8\div110$），$9500\div11364\approx0.84$

所以该网络的正常吞吐率（goodput）值是0.84。

21. 一大批ALOHA用户每秒产生50次请求，包括初始请求和重传的请求。时间以40毫秒为单位分槽

（a）首次尝试的成功率是多少？

（b）k次冲突后成功的概率是多少？

（c）所需要的发送尝试的次数的期望值是多少？

解答：（a）在任一帧时内生成k帧的概率服从泊松分布

$$p_r[k]=\frac{G^k e^{-G}}{k!}$$

生成0帧的概率为e^{-G}

对于纯ALOHA，发送一帧的冲突危险区为两个帧时，在两帧内无其它帧发送的概率为$e^{-G}\cdot e^{-G}=e^{-2G}$

对于分槽ALOHA，由于冲突危险区减少为原来的一半，任一帧时内无其它帧发送的概率是e^{-G}。

现在时槽长度为40毫秒，即每秒25个时槽，产生50次请求，所以每个时槽产生两个请求，G=2。因此，首次尝试的成功率是

$e^{-2}=1/e^2$

（b）$(1-e^{-G})^k e^{-G}=(1-e^{-2})^k e^{-2}=0.135\times(1-0.135)^k=0.135\times0.865^k$

（c）尝试k次才能发送成功的概率（即前k-1次冲突，第k次才成功）为：

$p_k=e^{-G}(1-e^{-G})^{k-1}$

那么每帧传送次数的数学期望为

$$E=\sum_{k=1}^{\infty}kp_k=\sum_{k=1}^{\infty}k\,e^{-G}\,(1-e^{-G})^{k-1}$$

$$=e^{G}=e^{2}\approx 7.4$$

22. 在一个无限用户的分槽ALOHA系统中，一个站点在冲突后到重传要等待的平均时槽数为4。请说明如何能够绘出此系统的时延对比吞吐率的曲线图。

解答：每帧传送次数的数学期望为：

$$E=\sum_{k=1}^{\infty}kp_k=\sum_{k=1}^{\infty}k\,e^{-G}\,(1-e^{-G})^{k-1}$$

$$=e^{G}$$

E个事件为E-1个长度等于4个时槽的间隔时间所分隔。因此一个帧从第一次发送开始时间到最后一次尝试成功的发送开始时间之间的长度即延迟是4（e^G-1），

吞吐率$S=Ge^{-G}$

对于每一个G值，都可以计算出对应的延迟值 $D=4（e^{G}-1）$，以及

吞吐率值 $S=Ge^{-G}$

按此方法即可画出时延对吞吐率的曲线。

23. 一个局域网采用Mok和Ward版本的二进制倒计数法。在某一时刻，10个站点的虚站号为8，2，4，5，1，7，3，6，9及0。要发送的下三个站点是上述序列中的4、3、9。当三个站点全部完成发送后，新的虚站号是什么？

解答：在解答这一问题之前，首先要了解什么是Mok和Ward版本的二进制倒计数法。在二进制倒计数法中，每个想要使用信道的站点首先将其地址以二进制位串的形式按照由高到低的顺序进行广播，并且假定所有地址的长度相同。为了避免冲突，必须进行仲裁：如果某站发现其地址中原本为0的高位被置换为1，那么它便放弃发送。对于次高位进行同样的信道竞争操作，直到最后只有一个站赢得信道为止。一个站点在赢得信道竞争后便可发送一帧，然后另一个信道竞争周期又将开始。Mok和Ward提出了二进制倒计数法的一个变种。该方法采用了并行接口而不是串行接口；还使用虚拟站号，在每次传输之后对站重新编号，从0开始，已成功传送的站被排在最后。如果总共有N个站，那么最大的虚拟站号是N-1。

在本题中，当4站发送时，它的号码变为0，而1、2和3站的号码都增1，10个站点的虚站号变为8，3，0，5，2，7，4，6，9，1

当3站发送时，它的号码变为0，而0、1和2站的号码都增1，10个站点的虚站号变为：

8，0，1，5，3，7，4，6，9，2

最后，当9站发送时，它变成0，所有其它站都增1，结果是

9，1，2，6，4，8，5，7，0，3.

24. 十六个站点正在竞争一条采用自适应树遍历协议的共享信道。如果地址编号为素数的站点突然全部准备发送，那么需要多少个时槽才能解决竞争？

解答：在自适应树遍历协议中，可以把站点组织成二叉树（参见图4-5）的形式。在一次成功的传输之后，在第一个竞争槽中，全部站都可以试图获得信道，如果仅其中之一需用信道，则发送成功。若发生冲突，则在第二槽内只有那些位于节点B以下的站（0到7）可以参加竞争。如其中之一获得信道，本帧后的时槽留给节点C以下的站；如果B点下面有两个或更多的站希望发送，在第二槽内会发生冲突，于是第三时槽内由D节点以下各站来竞争信道。

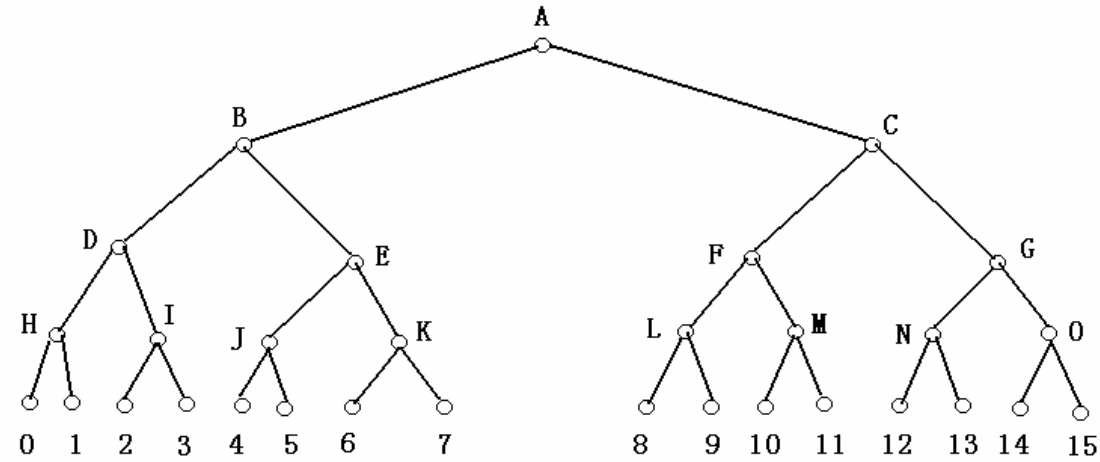


图 4-5　习题 24 插图

在本题中，站2、3、5、7、11和13要发送，需要13个时槽，每个时槽内参加竞争的站的列表如下：

第1时槽：2，3，5，7，11，13
第2时槽：2，3，5，7
第3时槽：2，3
第4时槽：空闲
第5时槽：2，3
第6时槽：2
第7时槽：3
第8时槽：5，7
第9时槽：5
第10时槽：7
第11时槽：11，13
第12时槽：11
第13时槽：13

25. 一个通过以太网发送的IP分组是60字节长（包括它的所有的头），如果不使用LLC, 那么在这个以太网帧中需要填充吗？如果需要，用多少字节？

解答：最小的以太网帧是64字节，包括在帧头中的两个地址、类型/长度域和检验和。由于头域占18字节，IP分组是60字节，总的帧长是78字节，已经超过64字节的最小值，因此不需要填充。

26. 一些书上说以太网帧的最大尺寸是1518字节，而不是1500字节。它们是错的吗？请解释你的答案。

解答：载荷是1500字节，但如果也算上目标地址、源地址、类型/长度和检验和段，总长度确实是1518字节。

27. 2^n个站使用自适应树遍历协议仲裁对一条共享线缆的访问。在某一时刻，它们之中仅有两个站准备发送。如果2^n 》1，那么遍历树的最小、最大和平均时槽数各是多少？
解答：2^n个站对应n+1级，其中0级有1个节点，1级有2个节点，。。。。，n级有2^n个节点。在i级的每个节点下面所包括的站的个数等于总站数的$1/2^i$。

本题中所需要的时槽数取决于为了到达准备好发送的两个站的共同先辈点必须往回走

多少级。让我们先计算这两个站具有共同的父节点的概率p_1。在2^n个站中，要发送的两个站共享一个指定的父节点的概率是

$$1 \div C_{2^n}^{2} = \frac{1}{2^{n-1}(2^n-1)}$$

总共2^{n-1}个父节点，所以，

$$p_1 = \frac{1}{2^{n-1}(2^n-1)} \cdot 2^{n-1} = \frac{1}{2^n-1}$$

$\because 2^n \gg 1$

$\therefore p_1 \approx 2^{-n}$

在共享父节点的条件下遍历树，从第2级开始每一级访问两个节点，这样遍历树所走过的节点总数$n_1=1+2+2+\ldots+2=1+2n$

接下来，我们考察两个发送站共享祖父节点的概率p2和遍历数所走过的节点总数n_2。此时在每个父节点下面仅可能有一个站发送。两个发送站共享一个指定的祖父节点的概率是

$$1 \div C_{2^n-1}^{2}$$

共有2^{n-2}个祖父节点，

$$p_2 = 2^{n-2} \div C_{2^n-1}^{2} = \frac{1}{2^{n-1}-1} \approx \frac{1}{2^n-1} = 2^{-n+1}$$

遍历树比n_1减少两个节点，即$n_2=1+2n-2=2n-1$

通过类似的分析和计算，可以得到，两个发送站共享曾祖父节点（属n-3级祖先节点）的概率是$p_3=2^{-n+2}$

遍历树所经过的节点总数比n_2又少两个节点，

$n_3=2n-1-2=2n-3$

.

.

.

$p_{i+1}=2^{-(n-i)}$

$n_{i+1}=2n+1-2i$

因此，最坏的情形是2n+1个时槽（共享父节点），对应于i=0；

最好的情形是3个时槽，对应于i=n-1（两个发送站分别位于左半树和右半树）

所以平均时槽数等于

$$m = \sum_{i=0}^{n-1} 2^{-(n-i)}(2n+1-2i)$$

该表达式可以化简为

$$m = (1-2^{-n})(2n+1) - 2^{-(n-1)} \sum_{i=0}^{n-1} i2^{i}$$

28. 1000Base-SX规范要求时钟运行在1250MHz，尽管千兆位以太网仅投送1Gbps的速率。这个更高的速率是为了提供额外的安全余地吗？如果不是，为什么要这样做呢？

解答：千兆位以太网在光纤上使用新的编码规则。1Gbps的曼彻斯特编码需要。2G波特的信号，这被认为是太困难了，而且也浪费带宽。取而代之的是在光纤通道上选择8B/10B编码。由于对每一个输入字节，都有1024（$=2^{10}$）个可能的输出码字，在选择什么样的码字方面就允许有一些灵活性。在做这种选择的时候，使用了下列两条规则：

（1）没有一个码字可以有连续的多于4个的相同的位。

（2）没有一个码字可以有多于6个的0或多于6个的1。

这些选择使得在位流中有足够的跳变，保证接收方跟发送方同步；同时也使得在光纤上0和1的个数尽可能地接近于相同。这样可减少直流成分的不良效应。

显然，1000Base-SX的编码效率是80%，它用10位发送数据表示8位实际数据。在1秒钟内发送1250兆位，即125兆个码字。每个码字表示8位数据，因此真正的数据速率确实是每秒1千兆位。

因此，本题的答案是否定的，即更高的速率不是为了提供额外的安全余地，原因如上所述。

29. 千兆位以太网每秒可以处理多少个帧？

解答：由于最小帧（64字节）可以用比传统以太网快100倍的速度发送，最大距离减少到1/100，变成25米。

802.3z委员会认为，25米距离是不可接受的。为了增加距离，在标准中引入了两个特征。第一个特征是载波延伸，在通常的帧之后让硬件加入填充，从而把帧延伸到512字节。由于填充是由发送方硬件加入、而由接收方去除的，软件并不感知，因此不需要改变现有的软件。当然，使用512字节发送46字节的用户数据，线路效率仅为9%.

第二个特征是帧迸发，允许一个发送方在单次发送中发送串接在一起的多个帧。如果总的迸发少于512字节，那么硬件还要做填充。如果有足够的帧在等待发送，这一方案是高效的，优于载波延伸。

上述两个新特征把网络的跨度延伸到200米，对于大多数办公室，可能都足够了。

最小的以太网帧是512位，因此以1 Gbps操作，每秒1 953 125帧，约每秒2百万个帧。

然而，仅当运行帧迸发时才能取得。没有帧迸发，把短帧填充到4096位；在这种情况下，最大数目是每秒244 140帧。对于最大帧1518字节，即12 144位，处理速率可达每秒82 345帧。

30. 举出两个可以把帧连续封装的网络。为什么说这种特征是有意义的？

解答：千兆位以太网可以这样做，802.16也可以这样做。这样做对于提高带宽效率（例如使用一个前缀等）；当对帧的尺寸有一个较低的限制时，这样做也是有益的。

31. 图4-6示出了基于MACAW(MACA for Wireless)的CSMA操作，并且使用虚拟通道感应。有四个站A、B、C和D。你认为在后面两个站中，哪一个最靠近A？为什么？

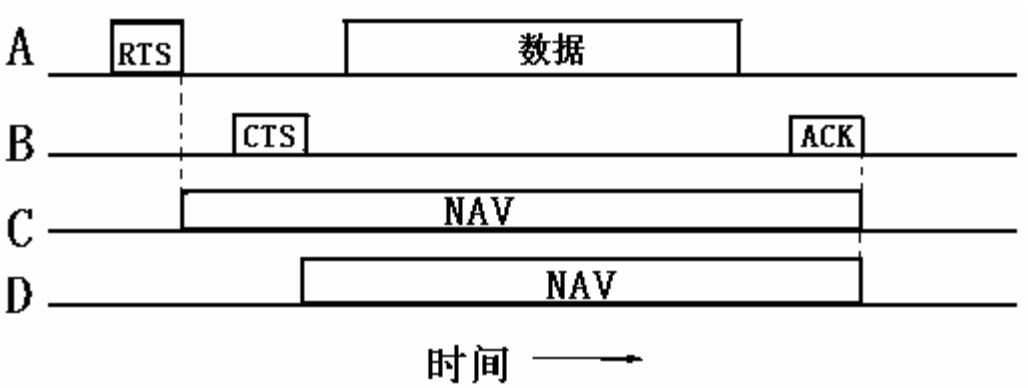


图 4-6　习题 31 插图

解答：站C最靠近A，因为它听到了RTS，并且通过宣告它的NAV(网络分配向量)作出相应。D没有必要对RTS作出相应，它一定是位于A的无线范围之外。

32. 假定一个11Mbps的802.11b LAN正在一个无线通道上连续地传输多个64字节的帧，位错率是10^{-7}。平均每秒有多少个帧被破坏？

解答：一个帧包含512位。位错率是10^{-7}。512位都传输正确的概率是

$(1-p)^{512} \approx 1-512p = 1-512\times10^{-7} = 0.9999488$

一个帧被破坏的概率等于

$1-0.9999488 \approx 1-0.99995 = 5\times10^{-5}$

每秒传输帧的数目等于$11\times10^{6} \div 512 = 21\ 484$

$21484\times5\times10^{-5} \approx 1$

因此，每秒大约有1个帧被破坏。

33. 一个802.16网络有一个20MHz宽的通道。可以给订户站发送多少个bps?

解答：由于随着到基站的距离的增大，信噪比下降，802.16采用了3种不同的调制方案。在本题中，如果订户离得比较近，使用QAM-64，20MHz带宽可得到$20\times6 = 120$Mbps的位速率。对于中等距离，使用QAM-16，可得到$20\times4 = 80$Mbps的位速率。对于较远的站，使用QPSK,可得到$20\times2 = 40$Mbps的位速率。

34. IEEE 802.16支持4个服务类别。对于非压缩视频的发送，使用哪个服务类别是最好的选择？

解答：IEEE 802.16支持的4个服务类别是：

- 恒定位速率服务；
- 实时可变位速率服务；
- 非实时的可变位速率服务；
- 尽力而为的服务。

非压缩视频有恒定的位速率。每个帧有跟前一帧相同数目的像素。因此可以非常精确地计算需要多大的带宽，以及在什么时候、什么情况下需要这样的带宽。所以在本题中，恒定位速率服务是最好的选择。

35. 给出两个理由，说明为什么网络可能要使用错误纠正码来代替错误检测和重传机制。

解答：一个理由是对实时服务质量的需求。如果发现了一个错误，没有时间允许用来重传。演示必须继续进行。在这种情况下就可以使用前向纠错。

另一个理由是在非常低质量的线路上（例如无线通道），错误率非常高，以至于实际上几乎所有的帧都必须重传，重传的帧也可能被破坏。为避免这种情况，可以使用前向纠错来增加正确到达帧的比例。

36. 图4-7示出，一个蓝牙设备可以同时在两个微微网中，为什么不可以让一个设备同时是两个微微网的主站呢？

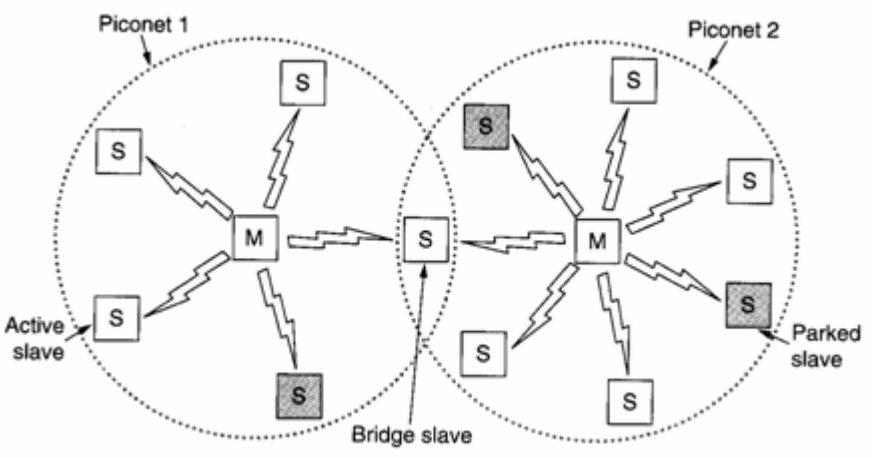


图 4-7　习题 36 插图

解答：一个设备同时是两个微微网的主站是不可能的。有两个问题。首先，在头端中仅有3个地址位，而在每个微微网中可能有多达7个从站。因此，一个问题是无法唯一地给每个从设备编址。

第二，在帧开头的访问码是从主站的标识得到的，通过这一方式从站说明哪个报文属于哪个微微网。如果两个重叠的微微网使用同一个访问码，将无法说明哪个帧属于哪个微微网。实际上，这两个微微网将会合并成一个大的微微网，而不是两个分开的微微网。

37. 图4-8示出多个802.11物理层协议。哪一个协议最接近蓝牙物理层协议？两者之间的最大的差别是什么?

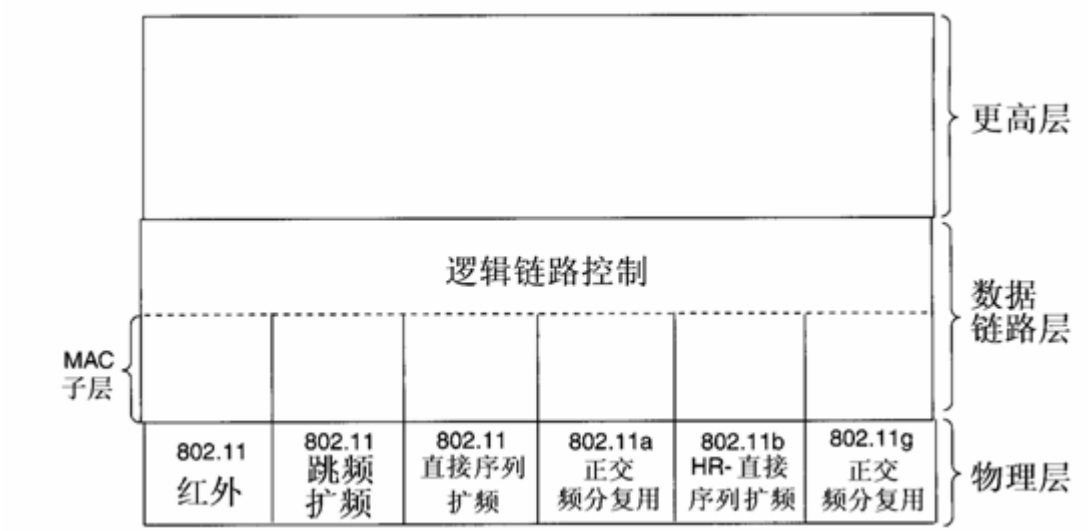


图 4-8　习题 37 插图

解答：蓝牙使用FHSS（跳频扩展频谱），802.11也使用FHSS。最大的差别是蓝牙跳变速率是每秒1600跳，而802.11在每一频率处停留的时间可以长达接近400毫秒。也就是说，蓝牙的跳变速率远远大于802.11。

38. 蓝牙在主站和从站之间支持两种类型的链路。它们是什么样的链路？分别用于什么样的目的？

解答：一种是ACL(异步无连接)通道，它是异步的，产生数据时帧不定期到达。另一种是SCO(同步面向连接)通道，它是同步的，帧以定义好的速率周期性到达。

39. 802.11的跳频扩频中的信标帧包含停留时间（指在每一跳的停留时间）。你认为在蓝牙中的模拟信标帧也包含停留时间吗？请解释你的答案。

解答：不包含。在802.11中的停留时间没有标准化，因此它必须向新到达的站通告。而在蓝牙中，停留时间总是625微秒（每秒1600跳），没有必要对停留时间进行宣告。所有的蓝牙设备都已经把此停留时间参数硬件化做入芯片了。蓝牙被设计成廉价的产品，固定跳变速率和停留时间，从而导致比较简单的芯片实现。

40. 考虑图4-9所示的互连LAN。假定主机a和b在LAN 1上，c在LAN 2上，d在LAN 8上。起初在所有桥接器中的散列表是空的，生成树如图（b）所示。说明在下列事件依次发生之后，不同桥接器的散列表是如何变化的。

（a）a给d发送　　（b）c给a发送
（c）d给c发送　　（c）d移动到LAN 6
（e）d给a发送

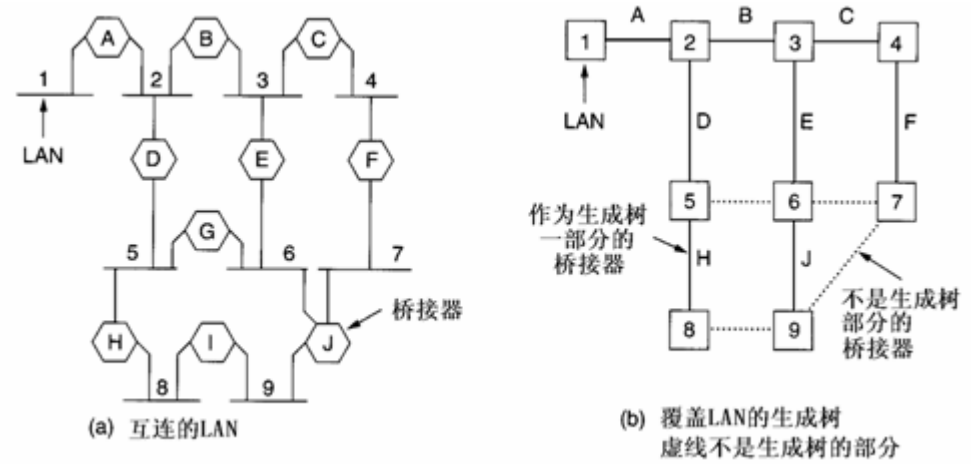


图 4-9　习题 40 插图

解答：第一个帧将被每一个桥接器转发。在这次传输之后，每个桥接器在其散列表中都有一个登录项列出目的地a和适当的端口。例如，D的散列表有一个登录项，用于在LAN 2上把帧转发到目的地a。第二个报文将被桥接器B、D和A看到。这些桥接器将在它们的散列表中附加一个将帧转发到c的登录项。例如，桥接器D的散列表现在又有一个登录项，表明如何在LAN 2上将帧转发前往目的地C。第三个报文将被桥接器H、D、A和B看到。这些桥接器将在它们的散列表中有一个把帧送往目的地d的新登录项。第五个报文将被桥接器E、C、B、D和A看到。桥接器E和C将在它们的散列表中有前往d的新登录项，而桥接器D、B和A将更新在它们的散列表中关于目的地d的登录项。

41. 在扩展LAN中使用生成树转发帧的一个结果是一些桥接器可能根本就不参与对帧的转发。请在图4-44中把这样的桥接器标识出来。有什么理由要把这些桥接器保持在那里吗？尽管它们没有被用于转发。

解答：桥接器G、I以及J的 LAN 6与 LAN 7之间的连接和 LAN 7 LAN 9之间的连接没有被用来转发帧。在配制连接中有回路的主要理由是增加可靠性。如果在现在的生成树中的任一桥接器实效了，动态的生成树算法会重新配置出新的生成树，该新的生成树可能包括上述桥接器中的一个或多个，现在它们就可能派上用场了。

42. 假定一个交换机的一块线路卡可以接4条输入线路。有时候一个帧从一块线路卡的一条线路上进入，并且从同一块线路卡的另一条线路输出。对于这种情况，交换机设计人员面对什么样的选择？

解答：最简单的选择是不做任何特别的处理。每一个输入帧都被送到底板，再输送到目的地卡，该目的地卡也可以是源卡。在这种情况下，在同一线路卡上输入和输出的交通

经过了交换机的底板。另一种选择对这种情况进行识别，对其做特殊处理，把帧直接发送出去，不让其通过底板。

43. 一台为快速以太网设计的交换机有一个可以移动10Gbps的底板。在最坏的情况下它能够每秒处理多少个帧？

解答：最坏的情况是有不断的64字节（512位）帧。如果底板可以处理10^9bps,每秒可以处理的帧的数目将等于

$10^9 \div 512 \approx 1\ 953\ 125$ 即1 953 125帧/秒。

44. 考虑图4-10(a)示出的网络。如果机器J突然变成白色了，那么对标记需要做改变吗？如果需要，怎样改变？

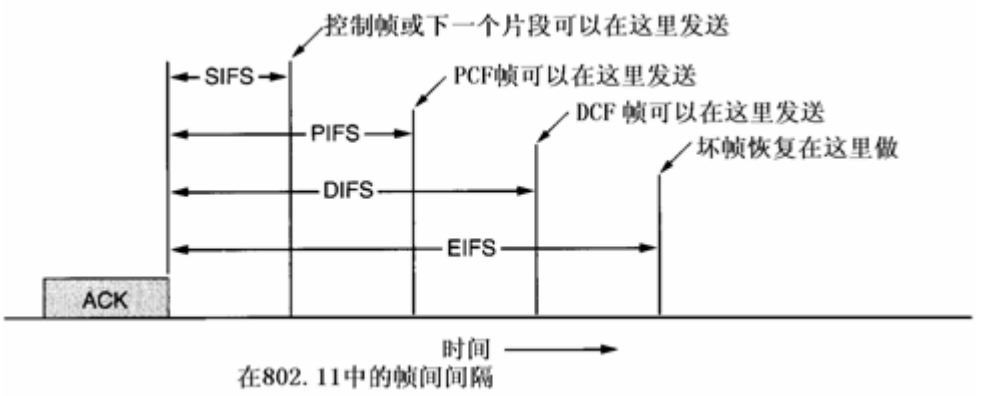


图 4-10　习题 44 插图

解答：需要把B1上前往LAN 3的端口重新标记成GW。

45．简要叙述存储转发交换机和直通交换机的差别。

解答：存储转发交换机先把每个输入帧整个地存储之后，再对它们做检查和转发。直通交换机在整个输入帧被全部地接收之前就开始对它进行转发，一旦接收完目标地址，就可以开始转发。

46．在处理被破坏的帧方面，存储转发交换机比直通交换机具有优越性。解释这是什么样的优越性。

解答：存储转发交换机在转发帧之前要把它全部存储下来。在一个帧进来之后可以验证其检验和。如果帧已经被破坏了，就立即把它抛弃。直通交换机不能够丢弃被破坏了的帧，因为当错误被发现时，帧已经被转发了。这就好比在马跑了之后再锁上马圈的门那样，为时太晚了。

47．为了使VLAN 能够工作，在交换机和桥接器中需要有配置表。如果在图4-11(a)中的VLAN使用的是Hub,不是多投点电缆，那么这些Hub中也需要有配置表吗？为什么？

解答：不需要。Hub只是在电气上把所有的输入线路连接在一起，没有配置工作需要

做。在Hub中没有路由选择。每一个进入Hub的帧，都会在所有其它的线路上输出。

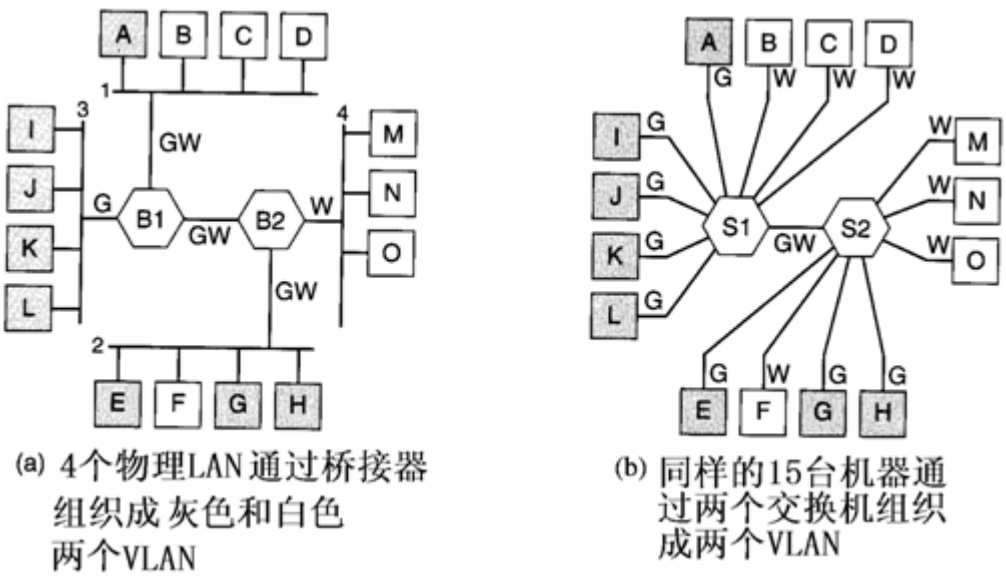


图 4-11　习题 47 插图

48. 在图4-12中，位于右边的传统端点域中的是一个感知VLAN的交换机。在这里可以使用一个传统交换机吗？如果可以，它是怎样工作的？如果不可以，为什么？

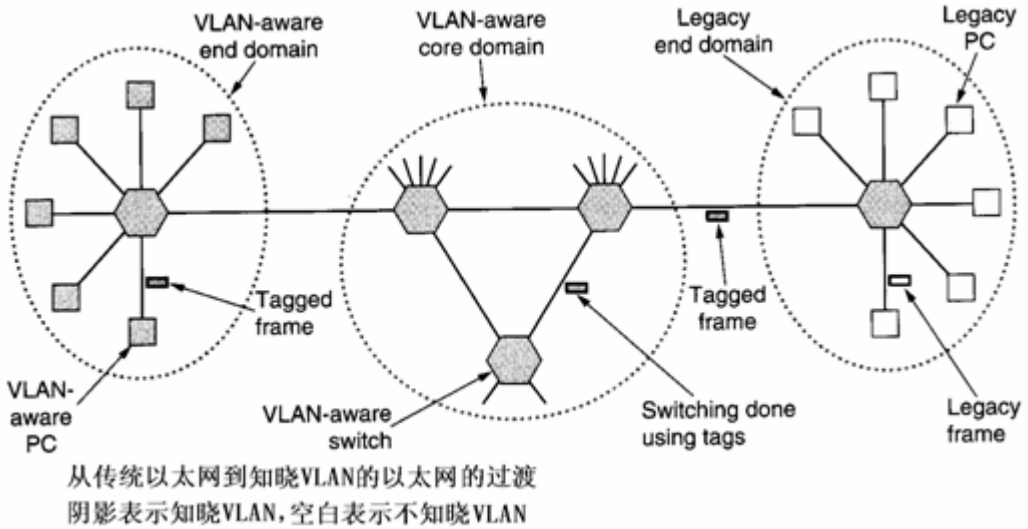


图 4-12　习题 48 插图

解答：它可以工作。进入核心域的帧将都是传统的帧，因此依赖第一个核心交换机对它们做标记。可以使用MAC地址或IP地址来做标记。类似地，在从核心域输出的方向上，那个核心交换机必须把输出帧的标记去除。

49. 一颗有两条上行链路和一条下行链路的卫星，假定缓冲区无限大，使用分槽

ALOHA信道能使下行链路的利用率达到0.736。问这个结果是怎么得到的？

解答：成功的概率（即在一个时间槽内正好有一个帧的概率）是1/e，约为0.368，那么，失败的概率（即无帧或多帧的概率）约为0.632。两个上行通道的结合概率如下：

链路1上成功且链路2上也成功的概率是0.135（=0.368×0.368）　　（发送2帧）
链路1上成功且链路2上失败的概率是0.233（=0.368×0.632）　　（发送1帧）
链路1上失败且链路2上成功的概率是0.233（=0.632×0.368）　　（发送1帧）
链路1上失败且链路2上也失败的概率是0.399（=0.632×0.632）　　（发送0帧）
那么，每个时间槽成功的期望值等于：
E=0.135×2+0.233×1+0.233×1+0.399×0=0.270+0.233+0.233=0.736.

50. WDMA和GSM两种信道访问协议的共同点是什么？

解答：WDMA是一个波分多路访问（wave length division multiple access）协议。每个站点分配2个信道；其中窄信道是控制信道，接收其它站发给该站的控制信号；宽信道用作该站点输出数据帧的信道。每个信道被划分成许多个时槽组。时槽0用某种特殊的方式标记，以便于后继时槽的识别。所有的信道均用同一个全局时钟来同步。每个站点都有2个发送端和2个接收端，它们分别是：

（1）一个波长固定不变的接收端，它用来侦听本站点的控制信道
（2）一个波长可调的发送端，它用于向其它站点的控制信道发送帧
（3）一个波长固定不变的发送端，它用于输出数据帧
（4）一个波长可调的接收端，它用来选择要侦听的数据发送端。

也就是说，每个站点都侦听自己的控制信道，看是否有请求产生，并将接收端的波长调为发送端的波长，从而得到数据。

GSM(global system for mobile communication)是一种数字蜂窝无线电系统信道分配方案。系统中每个蜂窝最多可拥有200多个全双工信道，每个信道包括下行链路频率（从基站到可移动站）和上行链路频率（从可移动站到基站），每个频段宽200k赫兹。每一个信道均可采用时分复用技术，支持多个独立的连接。

两种协议都使用FDM和TDM的结合方法，它们都可提供专用的频道（波长），并且都划分时槽，实现TDM。

51. 如果采用图4-13所示的GSM帧结构，那么用户发送数据帧的频度是多少？

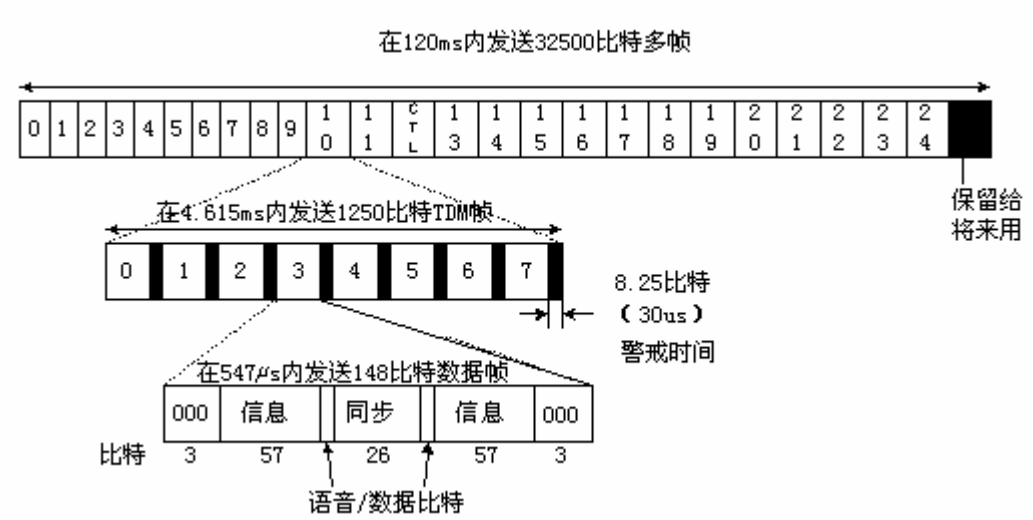


图 4-13　GSM 分帧结构的一个简化模型

解答：从图中可以看出，26个TDM帧构成1个120ms的多帧，8个数据帧构成1个TDM帧。每个信道的总速率都是在8个用户中均分。在每个TDM帧时内，每个用户都可以发送1个148比特的数据帧。因此每隔4.615毫秒（即一个TDM帧时）一个用户可以发送57位的突发数据块（在一个帧时内）。

综上所述，用户发送数据帧的频度是每个用户每4.615毫秒发送一个数据帧。

52. 假定A、B和C站使用CDMA（码分多址）系统同时发送比特0，它们的碎片序列如下：

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）

问发送结果产生的碎片序列是什么？

解答：首先对三个碎片序列求补

$$\overline{A}: (+1\ +1\ +1\ -1\ -1\ +1\ -1\ -1)$$

$$\overline{B}: (+1\ +1\ -1\ +1\ -1\ -1\ -1\ +1)$$

$$\overline{C}: (+1\ -1\ +1\ -1\ -1\ -1\ +1\ +1)$$

然后得到，

$$\overline{A} + \overline{B} + \overline{C} = (+3+1+1-1-3-1-1+1)$$

53. 在关于CDMA碎片序列的正交特性中，如果$S \cdot T = 0$，那么$S \cdot \overline{T} = 0$。请证明这一点。

解答：按照定义

$$S \cdot T \equiv \frac{1}{m} \sum_{i=1}^{m} S_i \cdot T_i$$

如果T站发送0而不是1，它的碎片序列被求补，第i个成分变成$-T_i$，那么

$$S \cdot \overline{T} \equiv \frac{1}{m} \sum_{i=1}^{m} S_i \cdot (-T_i) = -\frac{1}{m} \sum_{i-1}^{m} S_i \cdot T_i = 0$$

54. 考虑另一种检查CDMA碎片序列正交性的方法。两个序列中的每个元素可以匹配，也可以不匹配。请借助于匹配和不匹配来表示碎片序列的正交性。

解答：当两个元素匹配时，它们的乘积是+1；当它们不匹配时，它们的乘积是-1。为了让和等于0，匹配的数目必须跟不匹配的数目相等，因此，两个碎片序列当有一半元素匹配另一半元素不匹配时，它们就是正交的。

55. 某个CDMA接收方收到一条如下所示的碎片系列：

（-1 +1 –3 +1 –1 –3 +1 +1）

假如碎片序列如下：

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）

那么，哪些站点发送了数据？每一站点发送了什么数位？

解答：只须计算4个常规的内标积

（-1+1-3+1-1-3+1+1）• （-1-1-1+1+1-1+1+1）/ 8 = 1

（-1+1-3+1-1-3+1+1）• （-1-1+1-1+1+1+1-1）/ 8 = -1

（-1+1-3+1-1-3+1+1）• （-1+1-1+1+1+1-1-1）/ 8 = 0

（-1+1-3+1-1-3+1+1）• （-1+1-1-1-1-1+1-1）/ 8 = 1

结果是A和D发送比特1，B发送比特0，C保持沉默。

56. 考虑建立一个巨型计算机互连，还使用HIPPI（高性能并行接口）方法，但采用现代技术。现在数据通路是64位宽，每10毫微秒可以发送一个字。该通道的带宽是多少？

解答：每10毫微妙传送一个64位的字，以这种速率，每秒传送10^8 个字，数据速率等于

64×10^8=6.4千兆位/秒

所以，该通道的带宽等于每秒6.4千兆位。

57. 一座七层办公楼的每层都有15个相互邻接的办公室。在各办公室的前墙上均有一终端插座，这些终端插座在垂直平面上形成一个矩形格栅，插座间垂直和水平间隔都是4米。假定在任一对插座之间（垂直方向、水平方向或对角线）都可以连一条直的电缆，那么采用

（a）中央有一个路由器的星型配置

（b）一个802.3 LAN

（c）环网（无线路中心）

连接所有的插座各需要多少米电缆？

解答：（a）假定从下往上把七层楼分别编号为1-7层。在星型配置中，路由器放在4层中间位置。到达7×15-1=104个场点中的每一个场点都需要有电缆。因此电缆的总长度等于

$$4\sum_{i=1}^{7}\sum_{j=1}^{15}\sqrt{(i-4)^2+(j-8)^2}$$

$$\approx 1832\text{（米）}$$

（b）对于802.3（10BASE5），每一层都需要56米水平电缆，再加上24米（=4×6）垂直方向电缆，所以总长度等于

56×7+24=416（米）

（c）一种方案是采用螺旋结构，线缆经过（1，1）（15，1）（15，7）（1，7）（1，2）（14，2）等，总长度等于：

$$56+52+48+36+40+48+56+20+12+4+8+16+24+\sqrt{44^2+12^2}\approx 466\text{（米）}$$

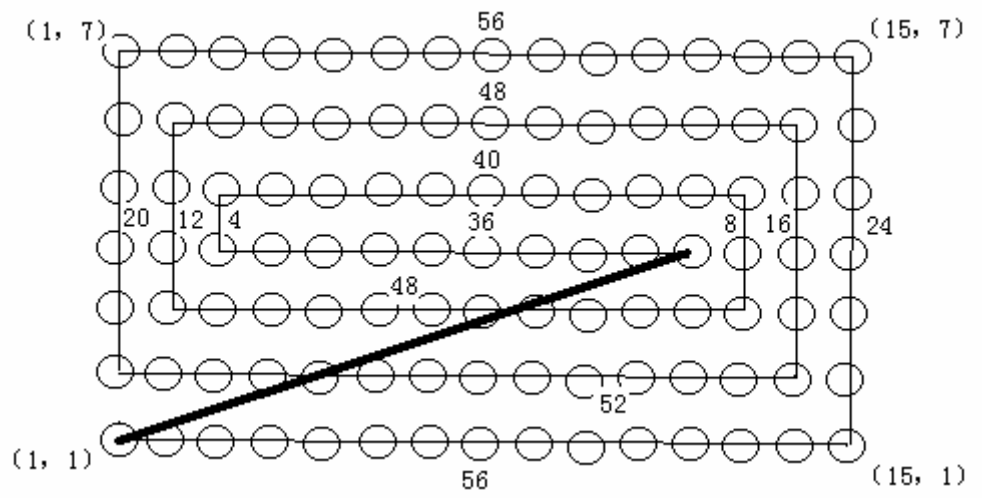


图 4-14　习题 57（c）插图

58. 一个1公里长的10Mbps的CSMA/CD局域网（不是802.3），其传播速度等于每微妙200米。数据帧的长度是256比特，其中包括用于帧头、检验和以及其它开销的32比特。传输成功后的第一个时槽被留给接收方，用来捕获信道并发送一个32比特的确认帧。假定没有冲突发生，有效数据速率（不包括开销）是多少？

解答：电缆的来回路程传播时间是10微妙（=1000÷200×2）。一个完整的传输有4个阶段：

发送方获取电缆（10微妙）

发送数据帧（25.6微妙）

接收方获取电缆（10微妙）

发送确认帧（3.2微妙）

4个阶段的时间总和是48.8微妙，在这期间共发送224个数据比特。

224÷48.8≈4.6Mbps。

因此，有效数据速率约为4.6Mbps。

59. 两个CSMA/CD站点都在试图发送长（多帧）文件。在发出每一帧后，它们采用二进制后退算法竞争信道。正好竞争k次便成功的概率是多少？每个竞争周期的平均竞争次数是多少？

解答：把获得通道的尝试从1开始编号。第i次尝试分布在2^{i-1}个时间槽中。因此，i次尝试碰撞的概率是$2^{-(i-1)}$，开头k-1次尝试失败，紧接着第k次尝试成功的概率是：

$$p_k = (1 - 2^{-(k-1)}) \prod_{i=1}^{k-1} 2^{-(i-1)}$$

该式可化简为

$p_k = (1-2^{-(k-1)})[2^{-0} \cdot 2^{-1} \cdot 2^{-2} \cdot \ldots \cdot 2^{-(k-2)}] = (1-2^{-(k-1)})2^{-(k-1)(k-2)/2}$

每个竞争周期的平均竞争次数是

$$\sum k\, p_k$$

60. 考虑建立一个CSMA/CD网，电缆长1公里，不使用重发器，运行速率为1Gbps。电缆中的信号速度是200000公里/秒。问最小帧长度是多少？

解答： 对于1公里电缆，单程传播时间为$1 \div 200000 = 5 \times 10^{-6}$秒，即5微妙，来回路程传播时间为$2\tau = 10$微妙。为了能够按照CSMA/CD工作，最小帧的发射时间不能小于10微妙。以1Gbps速率工作，10微妙可以发送的比特数等于：

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

因此，最小帧是10000位或1250字节长。

61. 一个令牌总线系统按如下方式工作：当令牌到达一个站点时，计时器重置为0。然后，该站点开始发送优先级为6的帧，直到计时器达到T6为止。随后，它开始发送优先级为4的帧，直到计时器计到T4为止。对于优先级为2和0的帧，也重复此算法，如果所有站点的T6到T0的计时值都分别是40ms，80ms，90ms和100ms，那么请问，预留给各优先级的带宽分别是总带宽的百分之几？

解答：四个优先级分别获得40、40、10和10毫秒，因此，总带宽的40%预留给优先级6，40%预留给优先级4，10%预留给优先级2，10%预留给优先级0。

62. 在令牌总线中，如果某站点接到令牌后即崩溃，将会发生什么情况？802.4协议是如何处理这种情况的？

解答：在一个站将令牌传出之后，它就观察它的后继站是否传出一帧或者交出令牌。如果二者均未发生，那么该站将再次传出令牌。如果第二次仍失败，该站就发送WHO_FOLLOWS帧，该帧中标明了后继站的地址。当崩溃站点的后继站看到WHO_FOLLOWS帧中给出的地址是自己的前站地址，它就发送SET_SUCCESSOR帧给出错站点的前方站点作为响应，声明自己将成为新的后继站。这样，出错的站点就从环中移去。

63. 当数据传输速率为5Mbps，且传播速度为200米 / 微妙时，令牌环接口中的一个比特时延等价于多少米的电缆？

解答：在5Mbps速率下，一个位时等于200毫微妙，在200毫微妙时间内信号可以传播的距离是$200 \times 10^{-3} \times 200 = 40$米

因此，令牌环接口中的一个比特延时等价于40米的电缆。

64. 令牌环网上的环时延必须能够容纳整个令牌。如果电缆不够长，必须人为地增加

时延。解释一下，为什么在时延只有16比特而令牌为24比特的环上，必须额外地增加时延？

解答：在发出16位之后，第1位又回来了，发送方不能让它继续绕环传输，因为令牌的发送还未结束。发送站可以在其内部人为地增加8位时延，在继续完成令牌发送的同时，缓存收到的8位，但此后，令牌中总会有8位通过发送站循环。在这种情况下，发送站不能发送更多的帧；并且只要令牌没有丢失，系统就不会崩溃。

65. 有一个重负荷的1公里长的10Mbps的令牌环网，其传播速率是每微妙200米，50个站空间上均匀绕环分布。数据帧256位，其中包括32位开销，确认应答捎带在数据帧上，因此是包括在数据帧内备用的位中，而不占用额外的时间。令牌是8位。请问，这个环的有效数据速率比CSMA/CD网高还是低？

解答：从获取到令牌的时刻开始计量，发送一个分组需要0.1×256=25.6微妙。此外，必须发送一个令牌，需要0.1×8=0.8微妙的时间。令牌必须传输20（=1000÷50）米，经过时间20÷200=0.1微妙才能到达下一站。此后，下一站又可以再发送数据帧。因此，我们在26.5（=25.6+0.8+0.1）微妙内发送了224（=256-32）位的数据，数据速率等于224÷26.5≈8.5Mbps，而10Mbps的CSMA/CD在重负荷50个站的情况下的有效数据率不超过3Mbps。显然，该令牌环网强于以太网的有效带宽。

66. 在令牌环网络中，发送方负责把帧从环上移走。如果改成让接收方除去帧，需要对系统作什么样的修改？这样做会产生什么样的后果？

解答：最大的问题是一位缓冲区不够了。在收到帧的第一位后，该站不知道是否应该吸收或转发该位，因此它必须有足够的缓冲区空间来存储帧，直到接收完地址段。作为这样做的结果，确认应答再也不能捎带给接收方。

67. 一个4Mbps的令牌环具有10毫秒的令牌保持计时值。在这个环上可以发送的最大帧有多长？

解答：以4Mbps速率工作，一个站在10毫秒内可以发送40000位或5000字节，这是帧的上限值。实际上，还必须从这个值减去一些开销字节，因此，数据部分的限值还要低一些。

68. 使用布线中心对于令牌环的性能是否会有什么影响？

解答：会有影响。我们知道，当令牌旋转时间增加时，令牌环网的性能减退。设立布线中心会增加总的电缆长度，因此也增加了令牌旋转时间。对于直径只有几公里的网络，影响较小；但对于一个大的都市网，影响可能是显著的。

69. 一个用作城域网的光纤令牌环长200公里，并且以100Mbps速率运行。在发送一帧之后，一个站在重新产生令牌之前把该帧从环上清除。在光纤中的信号传播速率是每秒20万公里，且最大帧长1000字节。问该环的最大效率是多少？（忽略所有其它的开销来源）。

解答：由环长200公里和传播速率每秒20万公里，可知1个比特绕环一周的传播时间是200÷（20×10^4）=10^{-3}秒，即1毫秒。发送速率是100Mbps，因此发送1个比特的时间是0.01微妙。发送最长帧1000字节需要的时间等于0.01×1000×8=80微妙，即0.08毫秒。当一个站

抓到了令牌时，它发送数据帧用0.08毫秒，然后等待最后1位绕环一周用1毫秒。当它再放出一个闲令牌时，下一站通过把令牌中的1个令牌位置1就可以立即把该令牌转换成一个常规数据帧的开头3个字节，从而又抓住了令牌，开始发送数据帧。

该站发送令牌所需的时间是：0.01×24=0.24微秒。忽略本站至下一站的传播时间，那么，在最坏的情况下，我们期望在1.080毫秒的时间内（将0.24微秒近似成0.000毫秒）发送8024比特（包括令牌24比特和数据分组8000比特）。这等效于8024÷（1.080×10^{-3}）≈7.4×10^{6}bps，即7.4Mbps的数据速率，不足10%的带宽利用率，可见效率是相当低的。

70. 许多人认为，以太网不适合实时计算，因为最坏情况的重传时间长度无上限。在什么条件下，该议论也适用于令牌环？在什么条件下，令牌环才会有一个已知的最坏情况？假定令牌环上站点的数目是固定的和已知的。

解答：在令牌环网上，如果一个站在抓取到令牌以后，保持令牌的时间不受限制，即它可以发送任意多个分组，那么，该令牌环网跟以太网一样，要发送数据的站点等待时间无上限。仅当每个站保持令牌的时间都有一个上限的条件下，令牌环网才是确定性的，即任何一站等待发送的时间都是有限的。

71. 以太网帧必须至少64字节长，才能保证在线缆的远端发生碰撞的情况下发送方仍然在发送。快速以太网同样有一个64字节的最小帧长规范，但位速率提高到了10倍。它是如何使得最小帧长规范能够维持不变的？

解答：快速以太网的最大线缆长度是以太网的1/10。

72. 假定有两个局域网桥接器，它们都连接到一对802.4网络。第一个桥接器每秒钟必须转发1000个512字节的帧。第二个桥接器每秒钟要转发200个4096字节的帧。你认为哪个桥接器需要更快的CPU？请讨论。

解答：每秒钟转发1000帧的桥接器需要比较快的CPU。虽然另一个桥接器有更高的吞吐率，但每秒转发1000帧的桥接器要处理更多的中断，更多的过程交换，传递更多的帧，需要CPU的其它各种处理工作也多。

73. 假定上题中的两个桥接器各自连接一个802.4 LAN和一个802.5 LAN，那么答案是否会改变？

解答：在802.4和802.5之间转发，情况有很大的差别。主要问题是需要颠倒所有字节的位的次序。这一操作是非常消耗CPU的。粗略估计，如果我们假定转换1个字节的顺序化1微妙的时间，那么这两个桥接器1秒钟内转换字节顺序的执行数目相差： 300k （≈4096×200-512×1000），即相差300毫秒的处理时间。尽管第二个桥接器由于每秒钟转发的帧的数目比第一个桥接器少800个，因而少处理800个中断，而且处理800个中断的时间比转换300k个字节顺序的时间是多是少还很难说，但有一点是肯定的，即情况大大不同了。

74. 在802.3 LAN和802.4 LAN 之间的桥接器存在断续的存储器错误的问题。这个问题会引起传送帧的错误不被检测到吗？或者说帧的检验和能够发现这些错误吗？

解答：工作在异类LAN之间的桥接器必须重新计算检验和，如果桥接器的存储器有故障，检验和又是针对存储在存储器中的帧计算，就会产生错误。假定不发生传输错误，到达目的地的帧将会有一个跟数据一致的检验和，但不同于源发帧的检验和（实际上数据也不同于源发方数据），因此可能出现发现不了的错误。

75. 一个大学的计算机系有3个以太网段，使用两个透明桥接器连接成一个线性网络。有一天，网络管理员离职了，仓促地请一个来自计算机中心的人替代，他的本行是IBM令牌环。这个新的管理员注意到网络的两个端头没有连接，随即订购了一个新的透明桥接器，把两个敞开的头都连到桥，形成一个闭合环。这样做之后会发生什么现象？

解答：不会出现什么特别的现象。新的桥接器在网上宣告自己的存在，生成树算法为新的配置计算一个生成树。新的拓扑会把其中的一个桥接器设置成备用方式，它将在其它桥接器失效的情况下投入工作。这种类型的配置以附加的代价提供附加的可靠性，但并非不正常。它不会引起任何问题，因为无论你连接多少个桥接器，结果你总是以生成树的形式运行网络。

76. 一个大的FDDI环有100个站，令牌环行时间是40毫秒。令牌保持时间是10毫秒。该环可取得的最大效率是多少？

解答：由于共有100个站，且环行时间是40毫秒，所以令牌在两个邻接站之间的传播时间是40/100，即0.4毫秒。这样一个站可以发送10毫秒，接着是0.4毫秒的间隙，在此期间令牌移动到下一站。因此最好情况的效率是：10÷（10+0.4）≈96%，即该环可取得的最大效率是96%.

77. 在FDDI网络中，一定数量的时间固定归同步数据业务所使用，多余的部分则可为异步数据业务所使用。图4-15中给出了一个包含4个站的环的例子，其中，TTRT（目标令牌旋转时间）等于15个帧长时间Sai（对i站的同步分配）等于3个帧长时间，对各个站都一样。TRT表示令牌旋转计时器的值，XMIT的值依次表示一个站发送的同步帧和异步帧的个数。假定帧长固定，并忽略其它各种延迟时间，试给出在图4-16中方框内x，y，z，u和v的值。

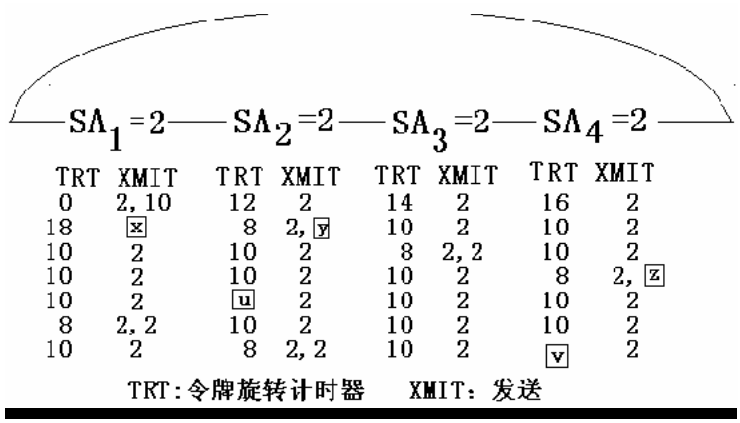


图 4-15　FDDI 传输量分配方案实施示例

解答：x=2,y=2,z=2,u=10,v=10。结果得到如图4-16所示的传输量分配数据。在开始时经历了一段无数据帧发送，因而开始时令牌旋转达到最快的速度，以至于当站1收到令牌时，它测得的TRT值为0。所以，它不仅能发送2个同步帧，还能发送10个异步帧。这里应记住令牌保持计时器（THT）需在送出同步帧后再开始工作。站2测得TRT值为12，但仍有权发送2个同步帧。

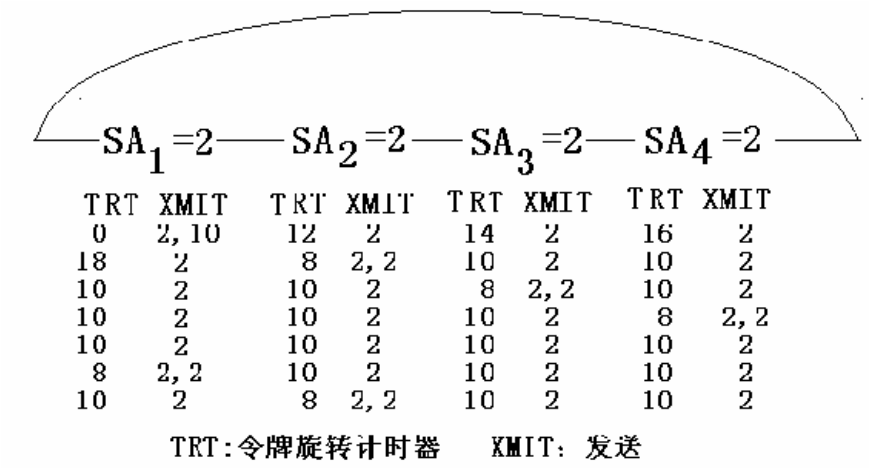


图 4-16　习题 77 答案插图

可以看出，如果每站继续发送最大允许的同步帧数，则TRT 值将上升到18，但很快稳定到10。在总的同步分配传输量为8和TRT为10的同时，异步传输的平均通信量为2。应该指出，如果所有的站永远存在积压的异步数据，那么这种发送机会将在它们之间轮流进行。

78. 假定信号在光纤中的延迟是每公里5微妙，试计算以时间和比特表示的下列FDDI环配置的延迟。假定可用的位速率是100Mbps。

（a）2公里环，带有20个站；
（b）20公里环，带有200个站；
（c）100公里环，带有500个站。

解答：设信号传播延迟等于Tp，一个站的延迟等于Ts，N表示站的数目，
那么环延迟T1 = Tp + N×Ts。在这里，Ts = 0.01微妙

（a）T1 = 2×5 + 20×0.01 = 10.2微妙，或1020比特
（b）T1 = 20×5 + 200×0.01 = 102微妙，或10200比特
（c）T1 = 100×5 + 500×0.01 = 505微妙，或50500比特

需要指出的是，上述值的计算是假定仅使用主环。如果发生了故障，将双环重构成单环，信号传播延迟值将加倍。而且，对于每个双附接站，站延迟也将加倍。

79. 1982年的以太网规范允许在任意两个站之间可以有长达1500米的同轴电缆、1000米的其它点到点连接线缆和两个重发器。每个站或重发器通过最长可达50米的分接电缆连接到同轴电缆。附表4-1列出了跟每种设备相关的典型延迟值（其中的c等于光在真空中的

速度3×10^8米/秒）

表4-1　跟每种设备相关的典型延迟值

条目	延迟
同轴电缆	传播速度　0.77c
链接 / 分接电缆	传播速度　0.65c
重发器	每个大约0.6微秒
收发器	每个大约0.2微秒

由于表中所列出的各种延迟，以比特为单位计量的最坏情况下的来回路程传播延迟是多少？

解答：单程延迟：

同轴电缆	1500米	6.49微妙
链接线缆	1000米	5.13微妙
重发器	两个	1.2微妙
收发器	六个（每个重发器两个，每个站一个）	1.2微妙
尾缆	6×50米	1.54微妙
		累计15.56微妙

来回路程延迟大约31.1微妙或311比特

标准允许的来回路程总延迟是464比特，加上48位的加强碰撞信号刚好等于512位的最小分组尺寸。

80. 为什么说以太网帧的长度段对于相邻上层（子层）是重要的？

解答：以太网有一个最小帧大小限制（对于10Mbps是64字节）；较小的分组必须加衬垫，以填充到最小帧大小。否则，把整个数据段的内容都递交给相邻上层，它将无法区分实际数据和填充。

81. 假定以太网的来回路程传播延迟是46.4微妙。这导致512比特的最小分组尺寸（464位的传播延迟+48位碰撞增强信号）。

（a）如果延迟时间保持常数，当信号速率上升到100Mbps时，最小分组大小将是多少？

解答：假定仍使用48位的JAM信号，那么最小分组尺寸将是

4640位+48位=4688位=586字节

（b）如此大的最小分组尺寸的缺点是什么？

解答：这个分组尺寸比许多高层分组尺寸大得多，产生相当数量的带宽浪费

（c）如果兼容性不是一个问题，怎样制定规范才能允许一个较小的最小分组尺寸？

解答：如果减少最大冲突域直径，并且其它各种容许量都很紧张，那么最小分组尺寸可以比较小。

82. 图4-17表示LAN通过网桥互连。请按照图上所标的网桥ID和端口号，利用生成树算法求出此网络的生成树。

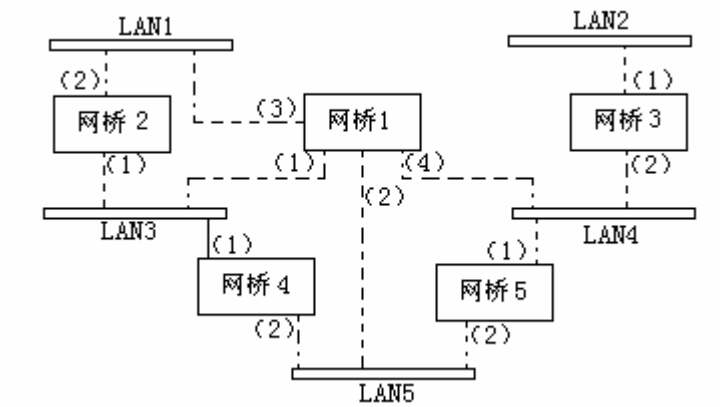


图 4-17　习题 82 插图 1

解答：

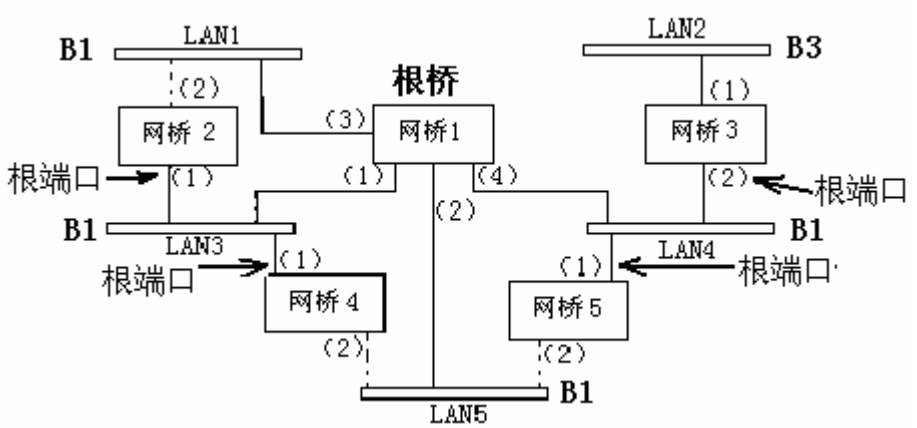


图 4-18　使用生成树算法配置后的拓扑结构

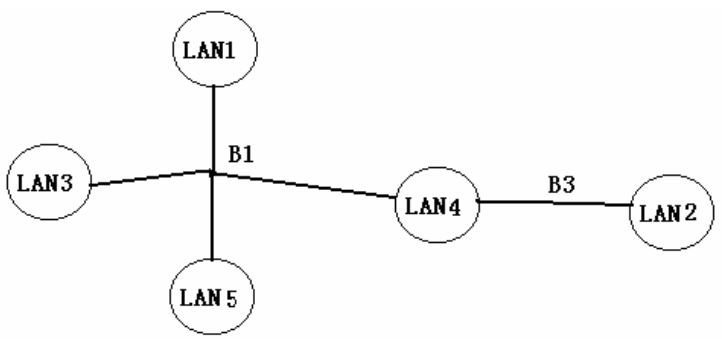


图 4-19　以 LAN 为结点以桥接器为弧的生成树图

83. 按照1982年以太网规范，在如图所示的典型配置中，在任意两个站之间允许最长

达1500米的同轴电缆（可以连接计算机），1000米其它的点到点链路线缆（仅用于网络范围延伸，不可连接计算机），以及两个重发器（也称中继器）。每个站或重发器通过最长可达50米的收发器电缆连接到收发器。跟每个部件相关的典型参数或延迟如下：
同轴电缆的传播速度为0.77c

链路/收发器电缆的传播速度为0.65c
每个重发器大约有0.6微妙的延迟
每个收发器大约有0.2微妙的延迟
其中c是光在真空中的传播速度，即3×10^8米/秒
由于上述延迟因素，以比特计的最坏来回路程延迟时间是多少？

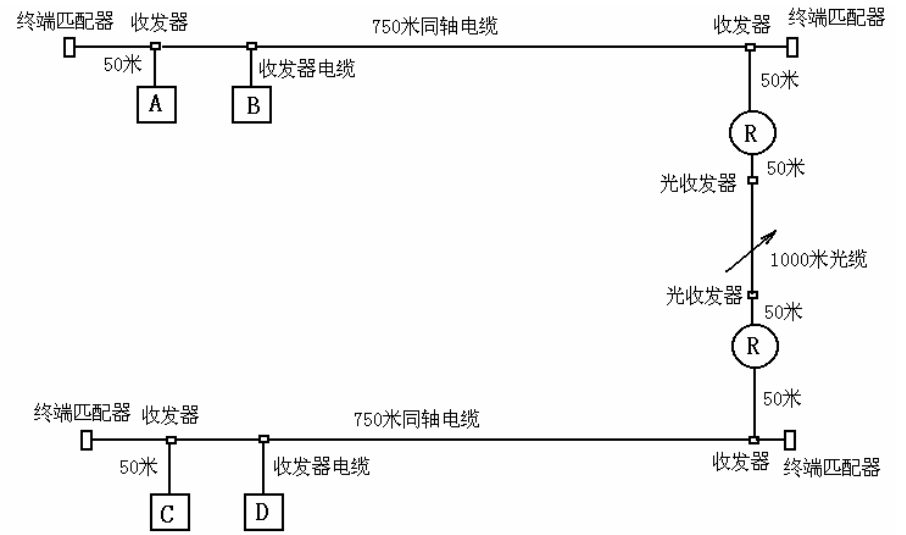


图 4-20　习题 83 插图

解答：单程延迟（例如，A到C）：

同轴电缆 6.49微妙（1500米）　　点到点链路 5.13微妙（1000米）
重发器 1.20微妙（两个）　　收发器 1.20微妙（6个）
收发器电缆 1.54微妙
总延迟　15.56微妙

来回路程延迟约31.1微妙，即311比特。再留有一定的余地，后来的正式标准是464比特，若再加上48比特的JAM信号，就导致最小帧长512比特。

84. IEEE802.3标准把在两个重发器之间的以太网同轴电缆段的最大长度限定为500米，重发器再生100%的原始信号幅度。下图示出的是一种典型的按照5-4-3-2-1黄金规则（5个段，4个重发器，3个网络段，2个链路段，1个冲突域）配置的网络。沿着500米的网络同轴电缆段，衰减后的信号不会低于原先值的14%，沿着1500米同轴电缆，衰减后的信号仍然可达原先值的$(0.14)^3=0.3\%$。在实践中，这样的信号在同轴电缆的接收站读出后还是足以区分其编码是什么样的二进制位串的。那么标准为什么把单个网络段的长度限制为500

米呢？

解答：一个站不仅在仅仅接收的情况下必须能够正确地检测到远方发来的信号，而且为了碰撞检测，在它自己发送的同时，也必须能够检测到远方站发来的信号，这就需要高得多的远方信号强度。

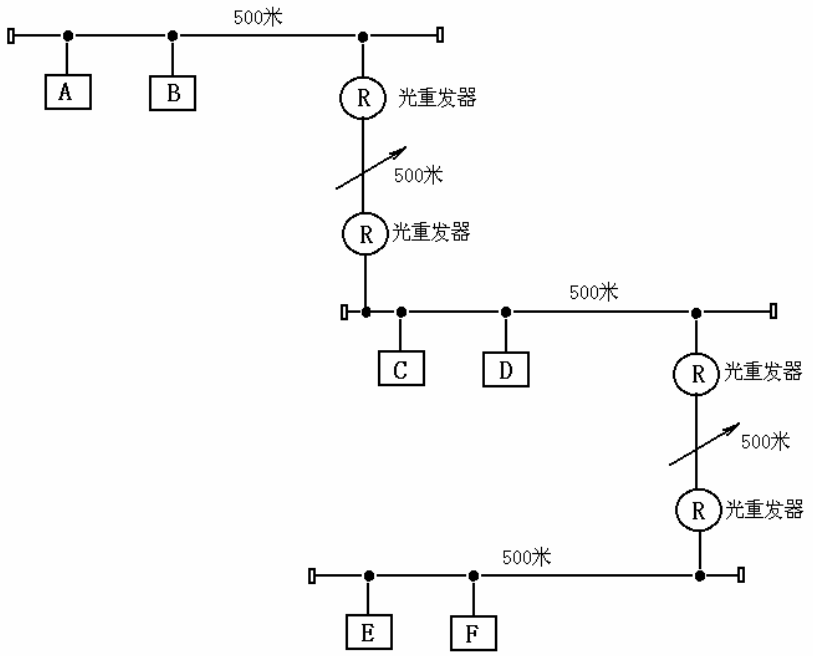


图 4-21　习题 84 插图

85. 假定A和B是试图在一个以太网上发送的两个站。每个站都有一个稳定的帧的队列准备发送，A的帧编号是A1，A2和A3等，B的帧编号是B1，B2和B3等。再假定指数后退的基本单元时间是T=51.2微妙。

现在A和B同时尝试发送1号帧，碰撞，并且刚好分别选择了0×T和1×T的退避时间，也就是说，A赢得了这一次竞争，发送A1，B需要等待。在这次传送结束时，B尝试再发送B1，而A则尝试发送A2。这一轮的首次尝试产生碰撞，此时，A的退避时间从0×T和1×T中选择，而B则从0×T，…，3×T中选择。

（a）给出A赢得第2次退避竞争的概率。

解答：A可以选择K_A=0或1；B可以选择K_B=0，1，2，3。如果（K_A，K_B）选择（0，1），（0，2），（0，3），（1，2），（1，3）中的一个组合，那么将是A赢得这第2次竞争，其概率是5/8。

（b）假定A已赢得了第2次退避竞争。A在成功发送A2后，接着尝试发送A3。当B再次尝试发送B1时，A和B再次碰撞。给出A赢得这第3次退避竞争的概率。

解答：现在A是在一次成功发送之后，可以选择K_A=0或1；K_B是在它的第3次碰撞之后，

可能的选择是0，1，2，…，7。如果K_A=0，那么K_B中有7种选择使得A赢；如果K_A=1，那么K_B中有6种选择使得A赢。所以A赢得这第3次竞争的概率是13/16。

（c）给出A赢得所有其余后退竞争的概率的合理下限值。

解答：A赢得第2次竞争的概率 = 5/8 > 1/2

A赢得第3次竞争的概率 = 13/16 > 3/4

类似地，A赢得第4次竞争的概率 > 7/8

一般地，A赢得第i次竞争的概率 > （$1-1/2^{i-1}$）

因此，假定A已经赢得第1至第3次竞争，那么A赢得所有其余的后退竞争的概率将不低于：

（1-1/8）×（1-1/16）×（1-1/32）×（1-1/64）×… ≈ 1-1/8-1/16-1/32-1/64- … = 6/8 = 3/4

（d）对于B1帧的发现会出现什么样的情况？

解答：B放弃对于B1帧的发送，转而开始发送B2帧。最终会因上层协议超时而重发B1帧的报文，从而恢复正常发送条件。

上述退避竞争的情况通常称为以太网捕获效应。

86. 假定对以太网发送算法作如下修改：在每一次成功的传送之后，主机在再次尝试发送之前等待一、两个时槽，在其它情况下仍按通常方式退避。

（a）说明为什么上题中所述的捕获效应现在发生的可能性要小得多。

解答：现在，如果A发送一个分组成功，由于必须等待一、两个时槽，那么B很有可能获得下一次发送机会。如果A和B是竞争通道的仅有的两个主机，那么现在很有可能让传送在两个站之间交替进行。

（b）说明该策略可能导致一对主机捕获以太网，它们交替发送，而同时封锁第3台主机。

解答：假定A、B和C三台主机竞争发送机会。我们假定A赢得第1次竞争，因此在第2轮竞争中，它向B和C退让两个时槽。开始，B和C碰撞；我们假定在1个时槽之后B先于C赢得通道（此时A仍处在退让期内）。当B结束其发送时，第3轮竞争开始。在这次竞争中B不参加（主动退让），由于C是同一帧发送的第3次退让，很可能A赢得通道。类似地，第4轮竞争中，B赢，C继续退让。

到这时候，C的退让范围很大；然而，A和B都很快成功，典型地在参与竞争的那个过程的第2次尝试就能成功，并且它们的退让范围被限定在1至2个时槽内。A和B在每次成功发送之后，彼此向对方退避1至2个时槽。很有可能，它们继续交替发送，直到C最后放弃。

（c）建议一种通过修改指数后退方式来避免上述现象发生的方法。

解答：可以通过增加一个站成功发送一个分组之后的退避时间来避免上述现象的发生。在试验过程中，相当于前述例子中A的站的逐步下降的平均成功率可用作修改后退时间长度参数的依据。

87. 现在假定以太网是运行p=0.33的p持续算法（即等待站在线路空闲时，以概率p立即

发送，以剩余的概率推迟51.2微妙的时槽）。当第4个站D正在发送的时候，作为尝试发送的一部分，假定站A、B和C都在做开始的载波感应。给出一种时序事件说明，表示可能的发送，尝试，碰撞和是否推迟的选择的序列。你的时序事件描述应该满足下列标准：（1）开始的发送尝试的顺序是A，B，C；但成功发送的顺序是C，B，A；（2）至少有一次碰撞，并且至少有一轮竞争中在空闲线路上产生4次退避。（可能有多种答案）

解答：
- A尝试发送；发现线路忙，等待；
- B尝试发送；发现线路忙，等待；
- C尝试发送；发现线路忙，等待；
- D发送完毕；
- 随后的第1个时槽，所有A、B、C三个站都后退（p=8/27）；
- 第2个时槽，A和B尝试发送（碰撞）；C后退；
- 第3个时槽，C发送（A和B都选择后退）；
- C完成发送；
- 随后第1个时槽，B尝试发送，A选择了后退，因此B竞争成功；
- B完成发送；
- 随后第1个时槽，A选择了后退；
- 第2个时槽，A选择了后退；
- 第3个时槽，A选择了后退；
- 第4个时槽，A第4次选择了后退（p=16/81≈20%）；
- 第5个时槽，A发送；
- A完成发送。

88. 假定有N个以太网站，它们都在同一时间尝试发送，需用N/2个时槽竞争确定谁赢得通道发送权。再假定平均分组大小是5个时槽，试把可用的带宽占总带宽的比例表示成N的函数。

解答：N/2个时槽的浪费带宽跟5个时槽的有用带宽交替发生，所以有用带宽占总带宽的比例等于5/（N/2+5）=10/（N+10）。

89. 在什么样的条件下如果没有监控程序，那么一个被破坏了的帧会在令牌环上无休止地循环？监控程序怎样才能克服这个问题？

解答：在正常条件下，当帧在循环回来的时候，发送者会把完成传送的帧删除。如果发送主机故障停机（形成孤儿帧），或者帧的源地址已被破坏，那么发送方将识别不了这个帧。

监控程序排除这种故障的方法是在帧第1次通过的时候把1个设置的监控位置1，当帧第2次通过监控站的时候（此时该帧肯定有问题）由监控程序将其删除。不管源地址是否被破坏，这种方法都能解决问题。

90. 一个IEEE 802.5令牌环有5个站，总的电缆长度是230米。监控站必须在环中插入多少位的延迟？针对4Mbps和16Mbps的令牌环网分别进行计算，并使用传播速率2.3×10^8米/

秒。

解答：由于当无站发送时，令牌连续地沿着环旋转，故环的比特长度最低极限必须与令牌长度一样（应是24位）。监控站的延迟缓存器必须保证：不管速率如何，绕整个环的时延不得小于24比特的时间。

230米/（2.3×10^8米/秒）=1微妙；在16Mbps环网上是16位。如果我们假定每个站引入最少1位的延迟，5个站附加5位。因此，监控站必须加上24-（16+5）=3位的附加延迟。在4Mbps的环网上，监控站需要附加24-（4+5）=15位延迟。

91. 考虑像FDDI那样的一个令牌环网，允许1个站保持令牌一段时间（令牌保持时间THT）。当所有的站都没有数据要发送时，令牌绕环一周所花的时间用RingLatency表示。

（a）用THT和RingLatency表示当只有1个站处于活动状态（有数据要发送）时的网络效率。

解答：THT/（THT+RingLatency）

（b）就网络效率而言，在一个时候仅有1个站处于活动状态（有数据要发送）时THT的最佳设置值是多少？

解答：无穷大。我们可以让该站发送它希望发送的任意长的数据。

（c）在有N个站处于活动状态（有数据要发送）的条件下，给出令牌旋转时间的一个上限值。

解答：TRT ≤ N×THT+ RingLatency

92. 考虑一个具有200微妙的环延迟的令牌环。假定使用令牌延迟释放策略，如果环具有4Mbps的带宽，那么可以取得的有效吞吐率是多少？如果环具有100Mbps的带宽，那么可以取得的有效吞吐率又是多少？请针对单个活动主机（有数据到发送）和许多个活动主机分别回答该问题。对于后者，有足够多的主机要发送数据，且忽略不计向前传递令牌所花的时间。分组大小为1KB（1024字节）。

解答：在4Mbps令牌环上，发送1个分组（8192位）花2毫秒的时间。单个活动主机发送2 000微妙后，接着令牌环绕引起200微妙空闲时间。所得到的效率是：

2000÷（2 000+200）≈91%

在这里，因为发送1个分组所花的时间超过环的延迟时间，当分组发送完毕时，分组的前面部分已经返回发送方，因此，立即的和推迟的令牌释放所产生的效果是相同的。

4Mbps×91%=3.64Mbps。

在100Mbps的令牌环上，发送1个分组要花82微妙（$8182\div100M\times10^6$）的时间。对于单个活动主机的情况，从一个分组开始发送起，经过200微妙分组返回；然后释放令牌，再等待200微妙令牌再次被得到，从而可以开始下一次分组发送。

82÷（200+200）≈20%　　100Mbps×20%=20Mbps。

对于有许多个活动主机的情况，每个站从一个分组开始发送起，经过200微妙分组返回；然后向前传递令牌（忽略不计这段时间），紧接着下一个要发送的站开始发送。

82÷200≈40%　　100Mbps×40%=40Mbps。

93. 有一个100Mbps令牌环网络，令牌旋转时间是200微妙，允许每个站在每次得到令牌时可以发送1个大小为1KB（1024字节）的分组。试计算任意一台主机可以取得的最大有效吞吐率。

（a）假定是立即令牌释放

解答：一台主机发送1个分组花82微妙的时间。它在发送完成时立即发送令牌；然后它可以再发送分组的最早时间也是在200微妙之后，因为此时令牌才可能再回到该主机站。

82÷（82+200）≈29%　　100Mbps×29%=29Mbps

因此，一台主机可以取得的最大有效吞吐率是29Mbps。

（b）假定是推迟释放令牌

解答：发送方在开始发送200微妙之后，帧的开始部分才能回到本站，此时发送方才发送令牌。令牌最早还要过200微妙的时间（假定其它站都不发送）才能饶环一周，回到该源发站，使该源发站可以再次发送。

82÷（200+200）≈20%　　100Mbps×20%=20Mbps

因此一台主机可以取得的最大有效吞吐率是20Mbps。

94. 假定一个100Mbps的推迟释放令牌的环网有10个站，环延迟是30微妙，协定的TTRT（目标令牌旋转时间）是350微妙。

（a）假定所有的站都被分配了相同数量的同步传输量，那么，每个站可以发送多少个同步帧字节？

解答：350-30=320微妙可用于帧传送，也就是32 000位或4k字节。在10个站之间均分，每个站400字节。

（b）假定站A，B，C在环上以递增的顺序排列。由于一致的同步交通，没有异步数据的TRT（令牌旋转时间）是300微妙。B发送一个200微妙（2.5k字节）的异步帧。那么A、B和C在它们下一次的测量中将看到什么样的TRT？下一次谁可以发送这样的一个帧？

解答：忽略不计在A、B、C之间的环路延迟。假定在时间T=0时B开始发送，那么

T= -300（微妙）令牌通过A，B，C；绕环一周；

T=0 令牌通过A；B抓住令牌，开始发送异步帧；

T=200 B结束发送，释放令牌；C看到令牌，C测量的TRT是500，此值太大，不能发送异步帧；

T=500 令牌返回到A，B，C；A测量的TRT是500；B测量的TRT也是500；C测量的TRT是300；

所以下一次C可以发送异步帧，因为它测量的TRT=300<TTRT=350。

95. 在一个以太网上，当第四个站正在发送的时候，作为尝试发送的一部分，假定站A、B、C都在做开始的载波感应。给出一种时序事件描述，表示一种可能的发送，尝试，碰撞和指数后退选择的序列。你的时序事件描述应该满足下列标准：

（1）开始的发送尝试的顺序是A，B，C；但成功发送的顺序是C，B，A；

（2）至少有4次碰撞

解答：下面给出的是一种可能的答案，当然，多种答案都是可能的。4次碰撞的概率看来相当低。可能发生的时间依次如下：

- A尝试发送，发现线路忙，等待。
- B尝试发送，发现线路忙，等待。
- C尝试发送，发现线路忙，等待。
- D发送完毕；A、B、C都检测到了这种情况，都尝试发送，碰撞。A选择K_A=1，B选择K_B=1，C选择K_C=1。
- 一个时槽之后，A、B、C都尝试再发送，再一次碰撞。A选择K_A=2，B选择K_B=3，C选择K_C=1。
- 一个时槽之后，C尝试发送，成功了。当C在发送时，A和C都尝试再发送，但发现线路忙，等待。
- C发送完毕；A和B尝试再发送，产生了第3次碰撞。A和B在这次碰撞后再退避，从同样的范围k<8中选择。假定A和B第4次碰撞（选择了同样的k），这次碰撞后，A选择K_A=15，B选择K_B=14。14个时槽之后，B发送。当B在发送时，A检测到这种情况（知道有一个站已赢了竞争），知道线路忙，等待B发送结束。

96. 假定以太网物理地址以随机的方式选择（使用真正的随机位）

（a）在一个有1000台主机的网络上两个地址相同的概率是多少？

解答：第2个地址必须不同于第1个，第3个地址必须不同于开头两个，第4个地址必须不同于开头3个，…，从第2个地址选择直到第1000个地址选择都不跟先前的选择冲突的概率等于：

$(1-1/2^{48})(1-2/2^{48})(1-3/2^{48})\ldots(1-999/2^{48})$

$\approx 1-(1+2+\ldots+999)/2^{48} = 1 - 999\,000/(2\times 2^{48})$

冲突的概率是$999\,000/(2\times 2^{48}) \approx 1.77\times 10^{-9}$

（b）在10^6个上述那样的网络中，有1个或多个网络发生上述地址冲突的概率是多少？

解答：$1.77\times 10^{-9}\times 10^6 = 1.77\times 10^{-3}$

（c）在（b）中描述的所有网络中，总共$(2^{10})^3 = 2^{30}$台主机之间某一对具有相同地址的概率是多少？

解答：使用（a）种得到的结果，产生冲突的大约概率等于：

$(1+2+\ldots+2^{30}-1)/2^{48} = 2^{30}\div 2\times(2^{30}-1)\div 2^{48} \approx (2^{30})^2\div(2\times 2^{48}) = 2^{11}$

显然该值已超出了有效范围，但说明冲突是肯定的。

第5章　网 络 层

本章学习重点

- 交换技术
- 路由选择算法
- 流控制
- 拥塞控制
- 资源分配

5.1　基本知识点

网络层的任务是把源计算机发出的信息分组经过适当的路径送到目的地计算机，从源端到目的端可能要经过若干中间节点。这一功能与数据链路层有很大的差别，数据链路层仅把数据帧从线缆或信道的一端传到另一端。因此，网络层是处理计算机网络中端到端数据传输的最低层。

网络层在其与运输层的接口上为运输层提供服务。这一接口是相当重要的，因为它往往是公共载体网络（例如IP网络)与用户的接口，也就是说，它是通信子网的边界。载体网络通常规定了从物理层直到网络层的各种协议和接口，它的工作是传输由其用户提供的分组。基于这种原因，对接口的定义必须十分明确和完善。

网络层的服务设计应该遵从三个原则。第一，服务与通信子网技术无关。第二，通信子网的数目、类型和拓扑结构对于运输层是遮蔽的。最后，运输层所能获得的网络地址应采用统一的编号方式，即使跨越多个LAN和WAN也应如此。

基于上述原则，网络层的设计者有相当大的自由度来编写提供给运输层的服务的技术规范。网络层的操作可以是面向连接的（例如ATM网络），也可以是无连接的（例如IP网络）。

为了实现网络层的功能，网络层必须知晓通信子网的拓扑结构（即所有路由器的位置），并通过子网选择适当的路径。选择路径时应该避免超载一部分通信链路和路由器，而另一些链路和节点却很空闲的现象发生。最后，当源端和目的端处在不同的网络中时，也应该由网络层来处理它们之间的差异，并解决由此带来的问题。

5.1.1　交换技术

在广域范围内，数据通信典型地是把数据从源节点经过中间交换节点的网络传送到目的地的。这些交换节点不关心数据的内容，它们的目的是提供在节点间移动数据的交换设

施，直到它们到达目的地。进行通信的端点设备可以被称作站。站可以是计算机、终端、电话或其它通信设备，我们把其目的是提供通信的交换设备称作节点，它们通过传输链路互相连接成一定的拓扑结构。每个站都附接到一个节点，所有节点的集合就称作一个通信网络。

在交换型通信网络中，从一个站进入网络的数据通过从节点到节点的交换，被选径送往目的地。一些节点仅仅连接到其它节点，这些节点唯一的任务是数据的内部(对该网络而言)交换。其它的节点连接了一个或多个站; 除了它们的交换功能，这些节点还从附接站接收数据，以及把数据投递给附接站。

节点到节点的链路通常是多路复用的，可以使用频分多路复用(FDM)，也可以使用时分多路复用（TDM）。网络一般都不是全连接，也就是说，并非在每一个可能的节点对之间都有一条直接链路。然而在网络的每一对站点之间总是希望有多于一条可能的通路，这样可以增加网络的可靠性。

在广域交换网络中使用两种相当不同的技术:电路交换和分组交换。这两种技术在沿着从源到目的地的通路上节点把信息从一条链路交换到另一条链路的方式有明显的差异。

使用电路交换的通信意味着在通信的两个站之间有一条专用的通信通路。该通路是连接在一起的一个网络节点间链路的序列。在能够进行通信以前，必须建立端到端（站到站）的电路。在电路的每条物理链路上都有一个逻辑通道专用于该电路。通常，电路交换的通信要经历三个阶段， 除了电路建立阶段，还有数据传输和电路释放阶段。

在分组交换网络中，数据以短的分组形式传送。典型的分组长度的上限是1000个字节(或称八位组)。如果一个源站有一个长的报文要发送，该报文就会被分割成一系列的分组。每个分组包含用户数据的一部分(或一个短的报文的全部)加上一些控制信息。控制信息至少要包括网络为了把分组送到目的地做路由选择所需要的信息。在路径上的每个节点，分组被接收，短时间存储，然而传递给下一节点。

分组交换根据其通信子网向端点系统提供的服务还可以进一步分成数据报和虚电路两种交换类型。在数据报分组交换中，每个分组的传送被单独处理，就像报文交换中的报文一样，但是若干个分组才构成一个报文，每个分组称为一个数据报。每个分组都有一个头，头中包含目标节点的地址，还包括顺序号，表明分组在报文中的位置。一个节点接收到一个数据报后，根据数据报中的地址信息和节点所存储的路由信息，找出一个合适的出路，把数据报原样地发送到下一节点。

在虚电路分组交换中，第1个分组决定随后所有分组都要遵从的路由。为了进行数据传输，网络的源节点与目的节点之间先建立一条逻辑通路，源端系统先向源节点发出呼叫请求，要求与目的端系统建立连接。源节点将该请求借助路由选择经过通信子网的中间节点送往目的地节点，目的地节点最后将请求送给目的地端系统。该呼叫请求是作为一个特殊的分组从源节点传送到目的地节点的。在虚电路建立起来之后，源端系统就可以向目的地端系统发送若干个数据分组。最后由源或目的地端系统发出折除连接的请求分组，这样整个连接就一段一段断开了。呼叫请求和拆除连接请求可能需要对方发回应答分组。

在交换型通信网中，一个端系统每次建立虚电路时，选择一个虚电路号分配给该虚电路，以便区别于本系统中的其它虚电路。在传送数据时，每个数据分组上不仅要有分组号、检验和等控制信息，还要有它要通过的虚电路的号码，以区别于其它虚电路上的分组。在

每个节点上都维持一张虚电路表，它的每一项记录了一个打开的虚电路的信息，包括虚电路号、前一节点和下一节点的标识。数据的传输是双向进行的，上述信息是在虚电路的建立过程中确定的。

5.1.2 路由选择算法

网络层的实质性功能是将信息分组从源端计算机选择路径送往目的地计算机。在绝大多数子网中，分组的整个旅程需要经过多个站段。

路由选择算法(routing algorithm)是网络层软件的一部份，它负责确定所收到分组应转发的外出链路。如果通信子网内部采用数据报，那么对收到的每个分组都要重新作路由选择。然而，如果子网内部采用虚电路，则当建立一条新的虚电路时，仅在开头作一次路由选择决策。以后，数据分组就通过这条已建立好的路由传送。后一种情形有时又称作会话路由选择(session routing)，因为在整个用户会话(例如终端上进行的登录会话或文件传送会话)期内都存在着一条路径。

为了实现自适应路由选择，需要有一个路由选择协议，以定义交换路由选择信息的方式和计算最短路径的方法，因为仅最短路径才被加到路由表格中。当前流行的路由选择协议基于两个重要的算法类型，即距离向量路由选择和链路状态路由选择。

5.1.2.1 Dijkstra 最短通路搜索算法

网络中的每条链路取决于路由判决标准而有不同的权值(Weight)，也称代价(cost)。若最佳路由考虑地理因素，则每个链路上的权值就是链路的长度；若考虑中继段数，则每个链路的权值都是1；有时也把链路上的容量考虑进去，链路权值与信道容量成反比，但与链路上的当前吞吐量成正比。

不管链路权值如何确定，最佳路由算法都基于下列原则：在全双工链路连接的网络上，每链路的每一方向上都有一个与之相关的权值。两个节点之间一条路由的代价是它所经过的链路权值之和，于是两个节点之间的最佳路由为这两个节点间所有可能路由中具有最小代价的那条路由。

在Dijkstra于1959年提出的求最短通路的算法中，首先为通信子网建立一个图，图中每个节点代表一个网络节点，每一条线代表一条通信链路，线上的标注表示两个相邻节点之间的权值。然后把每个节点用从源节点沿已知最佳路径到本节点的代价或距离来标注(放在圆括号内)。开始，一条路径也不知道，故所有节点都标注为∞。随着算法的进行和不断找到了路径，标注随之改变，使之反映较好的路径。一个标注可以是暂时性的，亦可以是永久性的。最初，所有的标注都是暂时性的。当发现标注代表了从源节点到该节点的最短可能路径时，就使它成为永久性的，不再进行修改。

当所有与工作节点相邻接的节点都已检查并且可能修改的临时标记都已经重新标注之后，这时便在全图的临时标记节点中找到具有最小标记值的节点。该节点变为永久节点，并且又成为下一个检查周期的工作节点。

整个过程中的每一循环都得出了当前从源节点到各目的地节点的路径及代价，直到扩大到所有节点。

为什么一个节点只要记录最佳路由上的下一节点而非所有节点呢？这是因为，在一条最佳路由上有一个最佳原理成立，即如果从节点A到节点B的最佳路由上经过了节点C，则在该最佳路由上从节点C到B的那一段也是从C到B的最佳路由，从A到C也如此，这是显而易见的。

5.1.2.2 距离向量路由选择

最早的也是相当简单的路由选择协议算法之一就是距离向量算法。在一个距离向量路由选择(Distance Vector Routing)协议中，所有的节点都定期地将它们的整个路由选择表传送给所有与之直接邻接的节点。这种路由选择表包含：

- 每条路径的目的地(另一节点)
- 路径的代价(也称距离)

术语“距离向量”起源于定期信息发送，一个报文包含有成对的列表(V，D)，这里的V表示目的地(叫做向量)，D是到达那个目的地的距离。注意距离向量是以第一人称报告路由的，即我们把一个节点送来的通告看成它在说：“我可以到达距离为D的目的地V”。在这种设计中的所有的节点都必须参与距离向量交换，以保证路由的有效性和一致性。

所有的节点都监听从其它节点传送来的路由选择更新信息。并在下列情况下更新它们的路由选择表：

- 被通告一条新的路径，该路由在本节点的路由表中不存在，此时本地系统加入这条新的路由。
- 通过发送来路由信息的节点有一条到达某个目的地的路由，该路由比当前使用的路由有较短的距离(较小的代价)。在这种情况下，就用经过发送路由信息的节点的新路由替换路由表中到达那目的地的现有路由。
- 在本节点的现有路由表中为了到达某一目的地首先应前往的下一节点如果通告了一个较高的代价，就要使用这一新的代价更新从本节点前往同一目的地的代价。

我们假定路由器知道它到每个相邻路由器的“距离”。如果度量标准是中继段数，距离就是1。如果度量标准是延迟时间，可以通过发送回送（ECHO）分组来测得（接收方会对分组加上时间标记后尽快返回)。作为一个例子，现在假定用延迟来作为度量标准，且路由器知道到每个邻居的延迟。每隔T毫秒，路由器把它估计的到达各个目的地的延迟的列表发送给每个邻居。它也从各个邻居那里收到类似的列表。假定从邻居X刚刚收到一个表，说明X路由器到达i路由器估计的延时是Xi，如果本路由器知道它到X的延迟是m毫秒，那么它也就知道通过X到达i路由器需要化（Xi+m）毫秒的时间。通过对每个相邻路由器进行类似的计算，本路由器就可以知道哪一个估计值最优，并且在它的新的路由选择表中使用这个估计值和相应的线路。注意，在计算过程中并不使用旧的路由选择表。

距离向量算法的主要缺点是网络规模的伸展性差。它对链路状态变化的响应慢，需要大尺寸的路由信息报文交换，并且报文的长度与通信子网内节点的个数成正比。由于距离向量协议需要每个存储转发的节点节点都参与路由信息的交换，因而交换信息的交通量也可能非常大。

距离向量算法的主要替代方案是一种叫“链路状态”（Link State）的算法，也称作“最短路径优先”（Shortest Path First），简称SPF。SPF算法要求每个参与协议的节点都有完全的网络拓扑信息，这里拓扑信息可以想象成每个节点都有一张地图，地图上标示了所有其它的节点以及它们所连接的链路。在抽象的术语中，网络节点对应于图中的节点，而连接节点的链路对应于边。当且仅当对应的节点可以直接通信时，在这两个节点之间才有一条边（链路）。

5.1.2.3 链路状态路由选择

参与SPF算法的节点不是发送含有所有目的地信息列表的报文，而是执行下述两项任务。第一，它主动测试所有邻接节点的状态。在图上，两个共享一条链接的节点是相邻节点。在网络术语中，两个相邻节点连接到同一条链路，或者连接到同一广播型物理网络。第二，它定期地将链路状态传播给所有其它的节点（或称路由选择节点）。

为了测试一个直接相连的节点的状态，一个节点定期地交换简短报文，询问该邻居是否是活动的和可达的，如果该邻居回答了，在它们之间的链路就称为是活动的。相反，如果收不到回答，就说它们之间的链路是不工作的。

为了通知所有其它的节点，每个节点定期地发出通告报文，该报文列出它所连接的每条链路的状态。这种状态报文并不描述路径，它只是报告它与哪些节点可以通过直接相连的链路通信。节点中的协议软件负责将每一链路状态报文投递给全网上所有参与SPF协议的路由节点。如果基础网络不支持广播，那么投递就通过点到点地转发一个个报文拷贝而得以实现。

简言之，在一个链路状态路由选择协议中，一个节点检查所有直接链路的状态，并将所得的状态信息发送给网上所有其它的节点，而不是仅仅送给那些直接相连的节点。以这种方式，每个节点从网上所有其它的节点接收包含直接链路状态的路由选择信息。

每当链路状态报文到达时，路由节点便使用这些状态信息去更新自己的网络拓扑和状态“视野图”，把各个链路标为“up”或“down”。一旦链路状态发生了变化，节点对更新了的网络图利用Dijkstra最短通路搜索算法重新计算路由。Dijkstra算法是从单一的报源出发计算到达所有目的节点的最短路径。

在链路状态路由选择算法中，每个节点都知道所有的节点分布在哪里，以及哪些链路将它们互连。每个节点都拥有关于整个网络的同样的视图。而且，路由更新报文相当短，因为它们仅包含直接链路的状态。

SPF算法的一个主要优点是，每个路由选择节点都使用同样的原始状态数据独立地计算路径；它们不依赖中间机器的计算。当一个节点从所有其它节点接收到了报文时，它可以在本地立即计算正确的通路，保证一步会聚。最后，由于链路状态报文仅运载来自单个节点关于直接链路的信息，其大小与网络中的路由节点数目无关；因此，SPF算法比距离向量算法有更好的规模可伸展性。

5.1.3 流控制、拥塞控制和资源分配

基本的承载服务是在一组路径上以指定的格式进行端到端的位流传输，这些服务在质

量、速度、延迟和差错等方面会有所不同。

一个源必须防止因发送报文太快使得接收方来不及存储或处理而产生溢出。流控制是使得接收方能够调整发送速率的一种机制。

端到端的延迟是一个固定的传播延迟和一个可变的队列延迟的和。为了保持这种延迟在可以接受的范围之内，必须控制分组进入网络的速率。拥塞控制是用于限制由一个源进入网络的分组数目的一组机制的通用术语。如果拥塞控制机制不能够正确地起作用，就可能有过量数目的分组在交换机的缓冲区中积累，引起不可接受的延迟或丢失。

一些应用需要网络能够保证提供不小于某个最小值的带宽，才能取得可以接受的性能。例如，话音会话需要64 kbps，而MPEG1需要1.5 Mbps。可变位速率应用将需要有保证的最小带宽和缓冲区的结合。因为网络资源——链路带宽和交换机缓冲区——同时被许多应用共享，就有必要设计资源分配机制，保证每个应用都能够得到所需要的资源，以维持其服务质量。

在发送方发送信息的速度比接收方能够处理的速度快的情况下，到达接收方的分组会因为缺乏缓冲区空间而丢失。流控制指的是为防止发送方淹没接收方缓冲区所采用的规程。

实施流控制最简单的规章是使用指示发送方停止发送信息的信号。假定A站正在以Rbps速率给B站发送。如果B站发觉它的缓冲区快要满了，它就给A站发送一个停止信号。在经过大约一个单程传播延迟Tprop后，A站停止发送，从B发送信号那一时刻开始，它还要接收2Tprop位，该数据量等于延迟跟链路带宽的乘积。因此，B站必须在它的缓冲区内容超过一个门槛值的时候就发送停止（OFF）信号。在终端和计算机之间的X-ON/X-OFF协议就使用这种类型的流控制。该协议也用在各种数据链路控制中。

ARQ滑动窗口协议也可以用来提供流控制。在最简单的情况下，发送窗口的大小WS等于接收方为发送方分组提供的缓冲区的数目。因为WS是发送方发出去的未得到应答的分组的最大数目，所以在接收方不可能发生溢出。当使用滑动窗口协议进行流控制的时候，对于每个分组的应答都可以看成是接收方发出的授权发送方发送另一个分组的信用量。

在使用超时重传机制的情况下，发送定时器的期满往往会引起我们不希望有的重传，这种情况说明了将同一机制（滑动窗口控制）用于不止一个目的 (错误控制或流控制)可能引起的限制条件。出于这种考虑，我们也要使用特别的控制分组指示发送方停止发送分组以及随后再继续发送分组。

我们还可以把对收到分组的应答跟给发送方发布信用量分开考虑。在这种方法中，我们在分组头中设置分离的域，分别用于分组的接收应答和发送信用量的发布。应答域仅说明已经收到了哪些信息，窗口大小由信用量域指定。实际上，接收方就是向发送方通告一个它准备接受的信息窗口。TCP采用的就是这种方法。

拥塞控制是指节制沿着一条通路的分组流保持网络部件免于变得过量拥挤所采用的控制规程。当来自多个源的位流被复用和读进一个交换机的缓冲区时，如果对源不加节制，缓冲区有的时候就可能被用尽，从而导致长的延迟，使缓冲区溢出和分组丢失。拥塞控制机制可以在监测到拥挤条件时让源减少注入到网络的分组的数目。

如果源采用回退N式选择性重传这样的窗口机制，那么，这种机制也可以被适当修改，用来服务于拥塞控制的目的。源可以从分组超时的现象发觉拥塞或分组丢失，因此，当有多个超时很快地连续发生时，源应该减少窗口尺寸。这种减少自动地降低了未得到应答的

分组数量，也就减少了网络拥塞。

在延迟带宽乘积大并且窗口也大的情况下，大多数尚未被应答的分组都在通过链路传播，而不是呆在缓冲区中等待。结果，当拥塞被发觉和减少窗口尺寸的时候，已经有许多分组在网络的链路上传输和被中转，减少窗口对这些分组不产生效应。它们继续到达缓冲区，增加拥塞和引起分组丢失。因此当连接具有大的带宽延迟乘积时，依靠窗口流控机制对拥塞控制的效果较差。

为解决这一问题，网络研究人员提出了基于速率的拥塞控制方法。该方法不是限制每个源注入到网络的分组数目，而是限制源发送分组的平均速率。这种控制机制易于实现，因为它仅要求每个源监视它的发送速率。

对于Internet，我们可以在UDP的顶部实现一个简单的基于速率的拥塞控制来代替TCP的基于窗口的拥塞控制。接收方发送一个报文给源，指定它希望源发送分组的速率。源通过计算和控制分组之间的时间实现这个速率。接收方可以计算什么时候应该收到这些被请求的分组。如果某个分组到达晚了，接收方可以给源发送一个修改的发送速率，比如说当前速率的一半。如果分组正常到达，那么接收方可以请求一个增加了的速率，比如说线性增加。为了防止请求丢失，在发出一定数目的分组之后如果没有收到来自接收方的报文，源应该停止发送。这种控制策略的一个优点是把计算速率更新的负担放到接收方，从而使服务器可以变得简单一些。

基于速率的拥塞控制的另一种实现是采用推荐给ATM网络使用的漏桶控制设施，它通过对输入源具有突发性的分组流做平滑化处理调节进入网络的交通。

不同的应用需要不同质量（延迟，差错率等）的承载服务。一个网络如果能够给一个应用专门分配资源（带宽、缓冲区），那么，它就能够保证为该应用提供一个特别的服务质量。

线路交换网络为每条连接专门分配一个固定的带宽，因此它能够为一个峰值速率小于该固定带宽的应用保证最小的延迟。

数据报网络是无连接的，网络交换机没有为区分来自不同应用的分组所需要的状态信息，因此该网络不能够为一个个可能有不同质量需求的应用专门分配资源。然而，在这类网络中实现某种粗略的资源分配机制也是可能的。例如，在Internet上，TCP协议(IP的上层)允许带有加快投递标志的分组得到比普通分组更高优先级的特别处理。作为另一个例子，交换机通过实现一个优先级或加权调度机制可以向不同类型的分组提供有区别的服务。

在虚电路交换网络中，每个分组都带有一个虚电路标识符（VCI）。这就允许交换机基于VCI对分组作不同的处理。在虚电路建立阶段，一个应用可以跟网络协商某种服务质量。然后网络交换机可以为该虚电路预留带宽和缓冲区，以提供协定的服务质量。因此在虚电路交换网络中是有可能保证服务质量的。

5.1.4 X.25公用数据网络

X-25协议是在国际上得到一致认可的建议书，定义了每个用户分组方式设备和网络节点之间交互的细节。用户分组方式设备和网络节点分别称作数据终端设备(DTE)和数据电路端接设备(DCE)。X-25协议独立于分组交换通信网络的内部结构。而且，非分组交换服务

必须使用装配/折卸(PAD)设施，例如，字符方式终端通过PAD连接到网络，后者将字符装配成分组。X-25协议基于层次概念，每一层都为下一个较高层次提供某些服务。这种结构不仅减少了设计复杂性，而且也为每一层掩盖了相邻层的实现细节。CCITT X-25建议书定义了三级通信，即物理级、链路级和分组级。

X-25接口建议提供对公用分组网络两种服务的访问。第1种是交换虚拟呼叫(SVC)服务。一个交换虚拟呼叫是在两个DTE之间的暂时的关联，并且由一个DTE给网络发送Call Request(呼叫请求)分组起始一个呼叫。第2种是永久虚电路(PVC)服务。一个永久虚电路是在两个DTE之间的一种长期存在的关联。永久虚电路设施不使用呼叫建立或清除过程，在某种意义上它类似于点到点的专有线路。事实上，虚呼叫就像通常打电话一样，建立连接，传送数据，然后释放连接。与此对比，永久虚电路就像租用的专线，它一直存在。每当两端中的任一端DTE想发送数据时，就只管发送，不用再建立连接。永久虚电路通常用在传输大量数据的情形。

X-25建议书由3级协议组成。它提供对虚呼叫和永久虚电路设施的访问，允许在同一条物理电路上一个DTE和网络上若干其它DTE之间进行多条连接的复用。这些逻辑连接中的每一条都利用在X-25的第3级定义的一条虚电路。所有三级接口互相独立，第1级和第2级可以被其它任何执行相同功能的协议代替。分组级对X-25接口是唯一的，它的替换将产生不同的接口。

X-25的3级协议通过DTE/DCE接口在本地闭合。这就意味着通过这3级接口的所有交换仅具有本地意义。然而，这些交换中的一些交换允许DTE向网络传递在网络传输系统内执行非本地操作所能完成的动作请求。

DTE通过一条数据电路访问分组交换设备。这可以是一条租用线路，或者是拨号连接；在许多情况下是利用电话网络中的模拟电路。数字电路的操作遵从CCITT的X-21建议书，该标准既提供了建立电路的快速数字寻址，也提供了对于租用电路的操作。适应过渡期内混合局面解决方案的需求又产生了X-21bis建议书，这个标准定义了用户通过模拟线路访问数字网络建立交换电路的寻址过程。X-21bis接口跟业已存在的V.24建议书兼容，V.24标准规定了DTE跟连接电话网的调 制解调器(modem)之间的接口。实际上，V.24就是EIA RS-232-C的对应CCITT版本。V.24和RS-232-C只是在某些很少使用的电路上有细微差别。V.25接口的第1层结合了X.21和X-21bis标准，以此规定了数据传输电路操作的电的和过程性特征。

X.25协议的链路级基于ISO发布的高级数据链路控制(HDLC)链路级规程。该链路级协议的主要责任是保证在DTE和DCE之间正确的数据交换。X.25已经定义了两个链路级协议；LAP(Link Access Procedure，链路访问过程)和LAPB(Link Access Procedure Balanced，链路访问过程平衡方式)。事实上CCITT采纳并修改了HDLC，形成LAP作为X.25的链路级标准，后来又修改成LAPB，使之与最后版本的HDLC更加兼容。现在人们更倾向于采用LAPB。LAPB在操作方式和监控帧方面区别于LAP。在LAPB协议中，每个数据帧运载单个分组通过X.25接口。链路级最有意义的功能是在DTE和网络之间提供无错的但可变时延的链路。

分组级协议使X.25具有对分组交换服务提供虚电路接口的特征。它提供建立虚电路然后发送和接收数据的设施。每条虚电路都可以使用一种窗口机制进行流控制。接口的错误恢复可以使用reset(重置)、clear(清除)和restart(重启动)过程。而且，正常的呼叫结束关闭虚

电路，以便它们可以用于其它呼叫。

X.25接口的分组级使用分组交织的统计型多路复用，在单个物理访问电路上建立并发虚电路形成若干逻辑通道，每一个都具有唯一的标识，可能的通道数是16个组，每组可以有256个通道。在每一个分组头中，使用4位标识组，使用8位标识通道。这些段中的二进制值表示组和通道号。在DTE和DCE的通道号之间有一一对应关系。能被DTE 使用的逻辑通道范围由网络管理机构指定。逻辑通道用以在分组交换网络上提供两种设施，即永久虚电路和虚呼叫。

一个DTE在同一时间可以有许多永久虚电路或虚呼叫在活动。这些呼叫将到达网络上许多其它DTE，与这些呼叫相关的分组都共享同一物理链路和第2级协议的错误控制过程。图6-13示出了这种数据流的多路复用。不管是什么样的网络内部结构，它都将从好几个DTE轮流把分组多路复用到它的节点之间的快速链路上。因此这些链路的带宽必须在活动网络用户之间共享，以使每个呼叫具有最小吞吐量保证。对于网络，保证源节点分组发送速率不能高于目的地分组接收速率也是很重要的。为此，每个逻辑通道都用窗口机制实现了流控措施。流控措施可供DTE使用，也可供DCE使用，从而网络用户可控制它接收数据流的速率。一个中断设施允许两个通过虚电路通信的DTE在中断分组中交换简短信息。这些中断分组可以在末端进程不能接受数据并且逻辑通道流已停止的条件下采用，作为化解问题的途径。

在一个关联(association)的两端只有清除一条逻辑通道中的流才能化解它们的问题的情况下，X.25提供了重置虚呼叫和永久虚电路的设施。reset(重置)操作清除所有数据分组通行的逻辑通道，并重新初始化流控制。restart(重启动)设施清除所有虚呼叫，并重置与一个特别DTE相关的永久虚电路。restart分组是唯一不载有逻辑通道标识的分组。网络本身在内部故障的情况下重置呼叫和重启动DTE。

数据分组的数据段可以是任意数量的位，不必是整数个字节，只要不超过网络限制的最大值即可。虽然可以选择16和1024之间以2为底的幂的任何数来定义以字节为单位的最大数据段长度，但X.25中优选的最大数据段长度是128字节。

5.1.5 ISDN和帧中继

ISDN（综合业务数字网）的意图是要建立一个世界范围的公用电信网络，用以代替现有的公用电信网，并且能够投递广泛种类的服务。ISDN通过用户接口的标准化进行定义，并且实现为一套数字交换机和通路，这些交换机和通路支持广泛的交通类型，并提供增值处理服务。实际上，在国家范围内存在着多重网络，但从用户的角度看，好像只有单个的可以访问的规格一致的网络。

ISDN已经被实现为一种进化性的技术，研制标准的委员会、公共载体部门和厂商联盟都理智地认识到，ISDN必须从业已存在的基于电话的集成数字网络（IDN）开始发展。结果，许多为T1和E1开发的数字技术被用于ISDN，这包括信令速率（例如32或64kbps），传输编码（例如双极性），甚至包括物理插头（例如电话插口）。因此ISDN的基础是在二十世纪七十年代发展起来的。

ISDN的用户接口是一个非常类似于X.25接口的拓扑结构。端点用户设备通过一种用户

—网络接口（UNI）协议连接到一个ISDN节点。当然，ISDN接口和X.25接口是用于两种不同的功能。X.25 UNI提供对分组交换数据网的连接，而ISDN提供对ISDN节点的连接，该节点又能够连接到一个话音、视频或数据网络。

ISDN一个显著的特征是从端到端通过整个网络保持用户信息和信令逻辑上分离。在ISDN用户系统中信息通道和信令通道是各自独立的。有关通信连接与释放的控制信息、呼叫过程中的控制信息等均通过D通道（信令通道）传输。因此在ISDN用户／网络间的协议中主要规定了D通道的控制规程。

ISDN网络的电路交换能力提供64kbps和大于64kbps的电路交换连接，用于用户信息传送。通信中的高层功能是由终端设备来提供的。

64kbps 的信息传送在 用户－网络接口的B通道上进行，和电路交换相关的控制信令在用户－网络接口的D通道上传送。窄带ISDN的电路交换能力是以64kbps交换为基础的。64kbps无交换能力则是通过64kbps电路的半固定连接实现的。大于64kbps的无交换能力可由多个64kbps电路半固定连接来实现。

B通道可以用于分组交换服务。在这种情况下，使用D通道控制协议，在B通道上在用户和分组交换节点之间建立一条电路交换连接。一旦在B通道上的电路建立起来了，用户就可以采用X.25的第2层和第3层在那个通道上建立一条通往另一用户的虚电路，并交换分组数据。

在D通道上的所有交通都采用称作 LAPD（链路访问协议－D通道）的链路层协议。LAPD协议基于HDLC，用户信息、协议控制信息和参数都在帧中传送。

典型地，每个用户设备分配一个唯一的终端端点标志（TEI，取值范围0~127）。单个设备分配多个TEI也是可能的，在终端集中器的情况下就是如此。

服务访问点标志(SAPI，取值范围0~63）)用于LAPD的第3层用户，并且对应在一个用户设备内的一个第3层协议实体。SAPI占用6比特，可在0－63范围内取值。值0用于管理B通道电路的呼叫控制过程（D通道协议第3层）；值16用于在D通道上使用X.25第3级的分组方式通信；值63用于诸如分配TEI这样的第2层管理信息交换。在32至61范围内的值用于支持帧中继连接。所有其它的值都保留为未来的标准化使用。

对用户来说，ISDN就是能够在一根普通电话线上实现可达到128Kbps的高速数据传送，可以同时处理话音、文字、数字、图象等多种信息。中国电信为ISDN业务取了一个形象的名字：“一线通”。

虽然ISDN的发展比较慢（从80年代初期开始），但在某些方面它还是很成功的。它以自己的LAPD 规范和Q.931消息协议卓越地服务于工业界。的确，这两个协议在通信工业界应用非常普遍。例如，LAPD是帧中继的一项基础技术，也是MODEM的链路访问规程(LAPM)的一项基础技术，而Q.931则在诸如移动无线电、帧中继和ATM等其它信令系统中广泛被采用。

总起来讲，作为公共服务电话网的一个发展，ISDN从本质上讲是电路交换的。但对于许多数据应用，显然是分组交换更为合适。然而，X.25不能适应ISDN保持用户信息和信令分离的模型。况且，在误码率比较低的数字环境中没有必要包括X.25持有的重型错误纠正协议。这就清楚地表明，在ISDN中需要某个另外的协议有效地支持数据服务。帧中继正是为了弥补这一空缺而诞生。

帧中继网络的目的是为端点用户提供一个高速虚拟专用网，能够支持有大的位速率传输需求的应用。与租用线路相比，它以较低的价格给用户以T1/E1访问速率。另外，帧中继的设计通过减少或删除在先前发展的数据网络（例如X.25）中执行的多种功能实现快速用户服务。 实际上，帧中继就是X.25在新的传输条件下的发展，是在ISDN标准化过程中在I.122建议中提出来的。它保存了X.25链路层HDLC帧格式，但不采用LAPB规程，而按照ISDN标准使用独立于用户数据信道的呼叫控制信令，即LAPD规程。它能够在链路层实现链路的复用和转接，而X.25则是在网络层实现复用和转接；也正因如此，帧中继可以完全不用网络层只用链路层（帧级）实现复用传送，故得名帧中继。

帧中继是一种简单的面向连接的虚电路分组服务。它既提供永久虚电路（PVC），又提供交换虚连接（SVC），并且遵从ISDN保持用户数据和信令分离的原则。

一条ISDN帧中继交换虚连接的建立方式与普通的电路型连接相同，并采用ISDN共路信令协议。与ISDN模型的区别在于数据传输或会话阶段，用户信息通过简单分组交换机（称为帧中继机）而不是电路型交叉点机制进行交换。

帧中继的设计消除了X.25加在端点用户系统和分组交换网络上的许多开销。下面列出的是帧中继和传统的X.25分组交换服务之间的主要差别：

- 呼叫控制信令在不同于用户数据的一条单独的逻辑连接上运载。因此，中间节点不需要在每条连接的基础上维持状态表或处理跟呼叫控制有关的消息。
- 逻辑连接的多路复用和交换发生在第2层，而不是第3层，这样就免除了一整个处理层次。
- 没有站段到站段的流量控制和错误控制。端到端的流控制和错误控制是高层的责任。

与X.25相比，我们失去了在一条条链路上做流量和错误控制的能力。在X.25中，多条虚电路在单个物理链路上运载，而且在从源到分组交换网，以及从分组交换网到目的地，LAPB可用来在链路段提供可靠传输。此外，在通过网络的每一跨段，也可以使用该链路控制协议来取得可靠性。使用帧中继，取消了按跳段进行的链路控制。然而，随着传输和交换设施可靠性的不断增加，这不是一个主要的缺点，况且还可以在高层提供端到端的流量和错误控制。

帧中继的优点是我们把通信过程流线化了。不论是在用户－网络接口，还是网络内部处理，所需要的协议功能都减少了。对照OSI参考模型，帧中继协议栈去掉了大部分的网络层功能和若干数据链路层的内容，而将其余的网络层功能下放到数据链路层；结果得到了低的延迟和高的吞叶率。研究表明，跟X.25相比，使用帧中继的吞吐率可以改善一个数量级或更多。使用帧中继的访问速率可以高达2Mbps。

用户通过（典型地）一个路由器或者某些其它的帧中继访问设备（FRAD)连接到帧中继网络。为了跟帧中继交换机通信，路由器实现了帧中继用户到网络接口（UNI）协议。虽然不排除把这个协议放在端点用户设备中的可能性，但是普遍的做法是对用户屏蔽帧中继的操作，从而向用户提供透明的数据传送服务。

如果帧中继的实现严格地遵从ANSI和ITU-T的标准，那么物理接口是基于ISDN的。然而现在的许多实现都使用T1/E1电路。帧中继规范还包括网络到网络（NNI）协议，该协议是由帧中继论坛颁布的。

在帧中继网络内部的操作和拓扑结构没有在任何帧中继标准中定义，也没有在帧中继论坛颁布的任何工作文件中加以说明。确实，NNI和UNI，正如它们的名字的含义那样，都是接口规范，帧中继网络提供者可以在网络内部自由地实现任何类型的协议、结构或其它参数。

支持帧中继承载服务的协议结构有两种分开的操作面，即控制(C)面和用户(U)面。控制面负责建立和终止逻辑连接，用户面负责在用户之间的用户数据传送。因此C面协议在用户和网络之间运行，而U面协议提供端到端的功能。

用于帧中继承载业务的控制面类似于在电路交换服务中的共路信令，有一个单独的逻辑通道用于控制信息。有一个单独的逻辑通道用于控制信息。在ISDN的情况下，控制信令在 D通道上传送，控制在B通道（或其它通道）上帧方式虚呼叫的建立和终止。在数据链路层，在用户（TE）和网络（ NT）之间的 D通道上使用LAPD（Q.921）提供带有错误控制和流控制的可靠的数据链路控制服务。这种数据链路服务被用来交换Q.933控制信令消息。

在端点用户之间实际的信息传送所使用的用户面协议是LAPF(Link Access Procedure for Frame-Mode Bearer Services)，该协议在Q.922中定义。Q.922是LAPD(Q.921)的一个增强版本。帧中继仅仅使用了LAPF的核心功能，包括：

- 帧的定界，定位和透明性；
- 使用地址段进行帧的多路复用和分离；
- 对帧进行检查，在传送前做0比特插入保证每个帧都由整数个字节组成，并在目的地接收后再做0比特抽出工作；
- 检查帧，保证它既不太长，也不太短；
- 检测传输差错；
- 拥挤控制功能。

上列最后一项功能是在LAPF中才有的，其余的功能也都是LAPD的功能。

在用户面中的LAPF核心功能是数据链路层的一个子层，它仅仅提供传送数据链路帧的服务，从一个用户到另一个用户，没有流量控制或错误控制。在此之上用户可以选择附加的数据链路或网络层以上的功能。这些都不是帧中继服务的内容。基于LAPF核心功能，帧中继网络提供具有下列性质的面向连接的链路层服务：

- 从网络的一边到另一边的帧传送保持顺序不变；
- 帧在传送中丢失的可能性小。

跟X.25类似，帧中继支持在单条链路上的多重连接。在帧中继的情况下，这些连接称作数据链路连接，并且每一条连接都有一个具唯一性的数据链路连接标识符（DLCI）。

LAPF核心协议在终端之间提供帧的保序的双向传输。它包括对帧的错误检测，但不纠正错误。这类网络也不进行流控操作，它将错误纠正和流控的任务留给在终端之间直接操作的高层协议去完成。因此网络节点对帧的处理很少，帧就可以很快地透明地通过网络。

在帧中继的帧格式的头部，其中有一位称作向前明确拥挤通告（FECN）位，还有1位叫做向后明确拥挤通告（BECN）位，它们被用来向用户终端运载拥挤指示。在前往接收

终端的帧中FECN位被置1，然后接收方可以使用高层协议让发送端减少它的发送速率，典型地是通过减少一个窗口大小。在返回发送终端的帧中BECN位被置1，并且更直接地获取同样的效果。

除了这些明确的拥挤指示，终端也可以从帧的丢失或跨越网络显著的时延中感应到拥挤。这有时被称作隐式拥挤通告。

除了明确的拥挤通告位，帧中继的帧头中还有第3位，叫做可以抛弃（DE：discard eligible）位，用户或网络可以将它设置成1，表示与该位没有被置1的帧相比，该帧在遭遇拥挤的情况下更可以优先被丢弃。

在帧中继出现之前，通过租用线路和X.25进行的局域网的广域互连方案是很昂贵的，特别是在国际互连的条件下，它们都与局域网的突发交通特征匹配不好。X.25是一个复杂的协议，易于对所运载的高层协议产生破坏性干扰，通常会严重地降低吞吐量。

帧中继的高速度和对高层协议的透明性使它成了在广域上互连局域网的理想选择。使用帧中继永久虚电路代替租用线路的等效安排。有两个重要的不同点，显示帧中继更为可取。首先，由于一条访问电路运载多个永久虚电路，每个路由器仅需一个广域接口，因此减少了路由器的成本。可以转向全部网状互连也是较有吸引力的，由于减少了需要规范路由器运载的中转交通量，故可以进一步降低路由器的成本。其次，仅仅在路由器和帧中继服务交换机之间的访问电路为用户专用。在帧中继交换机之间的电路与许多其他用户统计式共享，使得实质性地减少传输价格成为可能。

5.1.6 宽带ISDN和ATM

N-ISDN曾经打算用一个既适合语音也适合非语音交通的数字系统代替模拟电话系统。就基本速率达成世界范围的接口标准协定被认为会导致对ISDN设备的大量用户需求，从而导致大量生产、规模经济和廉价的VLSI ISDN芯片。不幸的是，标准化过程花了好几年的时间，在这一领域的技术变化很迅速，以致于标准一旦最后达成了，也就已经是过时的了。

当ITU-T最终意识到窄带ISDN不会做出什么惊人之举的时候，它试图设想一种新的服务。其结果就是宽带ISDN(B-ISDN)，当前的主要成分是用于从源到目的地以155Mbps速率移动固定长度分组(信元)的一条数字虚电路。由于这个数据速率足以支持(非压缩的)高清晰度电视，它很有可能至少在今后若干年内满足最大的带宽要求。

宽带ISDN基于异步传输方式(ATM：Asynchronous Transfer Mode)技术。ATM基本上是一种分组交换技术，而不是电路交换技术(虽然它能够相当好地仿真电路交换)。与此相比，现有的PSTN(公共服务电话网)和窄带ISDN都是电路交换技术。在电路交换中积累起来的大量的工程经验会由于改用ATM而变得过时无用。

宽带ISDN不能够在现存的电话用双绞线上传输实际应用所需要的距离。这就意味着采用宽带ISDN需要拆除大多数本地回路，铺设5类双绞线或光纤线路。而且空分和时分交换机不能用于分组交换，它们将必须被新的基于不同原理的以高得多的速率运行的交换机替换。唯一能够保留的东西就是广域光纤干线。

ITU-T把B-ISDN定义为需要能够支持大于一次群速率的传输通道的服务。B- ISDN在许多方面都跟N- ISDN(窄带ISDN) 不同。为了满足高清晰度电视的需求，需要大约150Mbps

的高通道速率。为了同时支持一个或多个交互性的分布式服务，需要大约600 Mbps总的用户线路速率。广泛支持这样的数据速率的仅有的适当的技术就是光导纤维。因此，B-ISDN的进展取决于光纤用户回路的采用步伐。

在网络内部，主要问题是所采用的交换技术。交换设备必须能够处理广大范围的不同位速率和交通参数(例如突发性)。尽管数字电路交换硬件的功能不断增加，光纤主干的使用也越来越多，但依赖电路交换技术处理B-ISDN大量的和多样的需求是困难的。由于这个原因，就需要采用某种类型的快速分组交换作为B-ISDN的基本交换技术，而且要求这种形式的交换容易在用户—网络接口支持ATM。

跟N-ISDN一样，B-ISDN的控制基于共路信令。在网络内部使用SS7增强支持高速网络的扩展功能。类似地，用户—网络控制信令协议是I.451/Q.931的一个增强版本。

当然B-ISDN必须支持窄带ISDN所支持的所有64Kbps传输服务，包括电路交换和分组交换;这样可以保护用户的投资，并且有利于从窄带ISDN向宽带ISDN过渡。宽带功能提供给高速数据传输服务;在用户——网络接口，这些功能将使用面向连接的异步传输方式(ATM)设施来提供。

1988年，CCITT兰皮书把ATM描述成一种基于非通道化的高速数字链路的交换技术。链路本身是全部基于光纤的点到点的干线，安排成每秒千兆位范围内的等级速度。这些在美国称作SONET(同步光纤网络)的光纤链路与ATM交换机相耦合形成新一代的网络，就是宽带ISDN。

ATM是英文“Asynchronous Transfer Mode”(异步传输方式)的缩写。这里的“异步”与PC MODEM通信中使用的术语“异步”不是一回事。在ATM中“异步”是指ATM取得它的非通道化带宽分配的方法。

ATM 是一种传输方式，在这种方式中，信息被组织成信元;说它是异步的，是因为包含来自一个特定用户的信息的信元的重复出现不必具有周期性。

ATM试图发明可以建造任何需要的或想要的种类的网的砖瓦。这种砖瓦就是ATM的信元(Cell)。ATM 中的许多信元技术都跟分组交换系统紧密相关，那就意味着，它是一种基于作为网络节点的交换机(而不是基于路由器)的面向连接的网络方法。

路由器和交换机都是网络设备，它们所执行的功能基本相同，即从一个输入端口得到一个数据单元，根据数据单元中头部的某个段查找一个表中的一个对应登录项，再把数据单元输出到该登录项指明的一个输出端口。二者的差别在于建立表的方法以及在数据单元头部的段中包含什么样的内容。在路由器中使用的是一个目标地址，而在交换机中则是一个连接标识符。有人说：“路由器是无连接的交换机，交换机是面向连接的路由器”，这种说法虽然有点夸张，但是并不过分。

在ATM网络中，网络节点(交换机)交换ATM信元。ATM信元结构由53字节组成，53字节被分成5字节的头部和称为载荷的48字节信息部分。这些字节在网络上一次一个字节地依次发送，从第1字节直到第53字节。由于信元的所有者不是由在数据流中的位置来决定，所以这里拥有者的确定是通过数据单元头部的一个功能得以实现的。

ATM是按需分配带宽。虽然ATM不能够凭空地产生带宽，但在多个用户共享带宽的情况下，它最灵活地使用可提供的带宽。

ATM有时称作标记多路复用，或异步时分多路复用。在标准研制阶段这两个术语都指

ATM，标记指连接标识符，告诉接收方该信元跟哪个连接相关联。

今天的大多数网络都采用一种数字数据链路技术，在某种线缆上传输数据。而且，大多数数字链路都是使用帧的传输，即有一些开销位或字节加到被传输的原始数据。这些载荷位加上开销位形成称为帧的一个单元。用于广域数字数据传输(例如T-1帧，T-3帧)的帧不同于我们通常在局域网上所使用的帧，为了发送方和接收方保持同步，并保证链路可用，必须连续不断地在物理上传输帧。数据被包装成传输帧(如果有数据的话)，或者没有数据时由发送方产生一种特别的空闲图案，并被接收方抛弃。各种各样的数据都可以被包装进这些传输帧。唯一真正的必要条件是接收方知道发送方发送的是什么东西，传输帧的一个可能的内容是ATM信元。

在大多数情况下帧以标准的速率产生，通常是每秒8000帧，或者每125μS产生一帧。由于ATM技术面向比现存网络速度更高的网络，ATM的数据链路比现有的常见数据链路的速度也要高。事实上，ATM是基于在美国称为SONET(同步光纤网络)的数字数据系列。SONET链路运行在51.84Mbps以及更高速率的光纤线缆上。51.84Mbps的链路称为STS-1（同步传输信号-1，电气规范—用于产生信号），155.52Mbps的链路称为STS-3C，在一个STS-1帧中，大约装载15个ATM信元，在一个STS-3C帧中将装载大约44个ATM信元。单个高速链路仍然可以用ATM信元来运载从用户到用户的任意小的带宽。这些信元流动形成在ATM中的一条连接，而不是在其它传输帧中(例如T-1)形成的通道。

ATM可以允许用户既能够以电路方式操作，也可以用分组方式操作。电路方式(语音是其典型的应用)也称恒定位速率(CBR)。分组方式(如数据应用)是可变位速率(VBR)。支持这两种方式的目的是现有网络设备和网络服务向后兼容。

在ATM中的逻辑连接称为虚通道连接(VCC)。一条虚通道连接类似于X.25中的虚电路或帧中继中的数据链路连接，它是ATM网络中的基本交换单位。虚通道连接通过网络在两个端点用户之间建立起来，然后在它上面交换可变速率的全双工的固定长度信元流。虚通道连接也用于用户——网络交流(控制信令)和网络——网络交流(网络管理和路由选择)。

ATM还采用了虚通路的概念。一条虚通路连接(VPC)是具有相同端点的一组虚通道连接(VCC)。因此，在单个VPC上的所有VCC上流过的所有信元被一起交换。ATM需要一种建立和释放虚通路连接和虚通道连接的机制。在这个过程所涉及的信息交换称作控制信令。

ATM的设计目标是要提供一种高速、低延迟、多路复用和交换的网络，集成语音、声频、视频和数据服务，并且通过减少交换操作的复杂度，减少在中间节点所需的处理，减少缓冲区管理的复杂性，以及减少在中间节点所需要的缓冲来匹配网络中高速传输的链路。

这些设计目标在高速传输的条件下，通过保持作为ATM传输基本单位的ATM信元在长度上短而固定而得以满足。保持短的单元长度得以在使用带宽的方式方面提供很大的灵活性。这种灵活性又为宽带ISDN(综合业务数字网)提供基本的框架，以支持正在涌现的各种应用程序所需要的广大范围的服务。而且，使用短的固定长度的信元有助于通过统计复用对传输缓冲区和带宽的高效利用。

ATM信元头部包含虚通路标识符(VPI)段，虚通道标识符(VCI)段，载荷类型(PT)段，信元丢弃优先级(CLP)段和头错误检查(HEC)段。在一个ATM端点站和ATM网络之间的分界点，信元头还包含一个一般流控(GFC)段。在ATM网络内部，这个4位的段是虚通路标识符的一部分。GFC(一般流控)是一个4位的段，它的使用是为了控制用户到网络的交通，而不

控制在相反方向上的交通(即从网络到用户的交通流)。另外，在网络内部不使用一般流控段。

ATM分层参考模型包括物理层、ATM层和ATM适配层。 总的说来, 这些层并不严格地对应OSI七层模型的相关层次。每一层又由一些相互不同的子层组成。

物理层将来自一个接口的信元通过一个传输通道传输给一个远程接口。物理层本身产生信元，并将信元插入传输通道，或者在没有ATM信元发送时填充通道，或者传递物理层操作和维护信息(这些信元不传递给ATM层)。

ATM 层是对信元进行多路复用和交换的层次。它在端点之间提供虚连接，并且维持协定的服务质量，在连接建立时执行连接许可控制进程，在连接进行当中监察达成的交通协定的履行情况。

ATM适配层，简称AAL(ATM Adaptation Layer)，允许各种网络层协议都可以使用ATM层的服务。ATM层仅支持OSI模型数据链路层的较低子层功能。因此，为了让网络层使用ATM，还需要一个填充子层。

AAL在用户所需要的服务(例如话音，视频，帧中继，X.25)和ATM层提供的ATM承载业务之间进行转换。它由会聚子层(CS：Convergence Sublayer)和分割与重组子层(SARS：Segmentation And Reassembly Sublayer) 组成。取决于所支持的实际业务，会聚子层执行多种多样的功能，包括时钟恢复，由网络引入的单元延迟差异的补偿，以及处理由网络引入的其它不利条件，比如信元丢失。分割与重组子层将用户信息和会聚子层所加的支持信息放在一起切片，以便适合相继的ATM 信元的载荷规范，能够通过网络传输；在传输的另一方向上，它重组用户信息，将用户信息恢复成在发送端分割前的样子。

服务质量对于ATM网络是一个非常重要的事项，其部分原因是因为它们用于诸如声频和视频这类实时交通。在建立一条虚电路的时候，端点用户(典型地是在主机中的一个进程，代表客户)和ATM网络层(代表网络运营者，或称载体部门)必须达成一个定义服务的协定。

ATM适配层的目标是向应用程序提供有用的服务，并且遮蔽在源端把数据分割为信元、在目的地又把信元重组为数据的机制。

开始, ITU—T定义了四个协议，分别是AAL1、AAL2、AAL3和AAL4。后来又把AAL3和AAL4合并为AAL3/4。然而，计算机工业界在实践中认识到所有这些协议都不能令人满意。作为权宜之计，又定义了另一个协议AAL5来解决这个问题。ALL-1是为恒定位速率服务定义的唯一的适配层，而其它所有的适配层都是为可变位速率服务定义的。

5.2 基本练习题

1. 选择题

当使用一个公用分组交换网络时，用户负责下列任务中的哪一种？

a. 把数据从源节点传输到目的地节点
b. 检查数据中的传输错误

c. 把数据加工成网络所期望的格式

d. 把数据划分成分组

解答：c.

2. 重传是如何使现存的拥塞问题变得更加严重的？

解答：当在已经发生拥塞的网络中有越来越多的分组得不到肯定应答时，发送方不断重传信息，这样就把更多的分组加到线路上，并使路由器的缓冲区被占满。

3. 试说明TCP是如何实现拥塞控制的？

解答：TCP拥塞控制算法根据网络状态动态地调节拥塞窗口。TCP拥塞控制算法的操作可以划分成3个阶段。第一阶段在算法启动或重启动时运行，并且假定管道是空的。该技术被称作慢启动，其执行是首先把拥塞窗口设置成一个最大尺寸的段，每当发送方接收到来自接收方的一个应答时，发送方把拥塞窗口增加一个段，在发出第一个段之后，如果发送方在超时之前接收到应答，发送方就把拥塞窗口增加到两个段。如果这两个段被应答，拥塞窗口增加到4个段，等等。在这一阶段拥塞窗口呈指数增长。指数增长的原因是慢启动需要尽快充满空的管道。

慢启动不会长久地增加拥塞窗口，因为管道最终将被充满。特别地，当拥塞窗口达到一个称作拥塞门槛的指定值（拥塞门槛起初被设置成65 535字节）时，慢启动停止。在这一点被拥塞避免阶段取而代之，这一阶段假定管道的运行接近被充分利用。在拥塞避免期间线性地而不是指数地增加拥塞窗口，其实现是对于每一往返时间增加拥塞窗口一个段。

显然，拥塞窗口不可以无限制地增加。当TCP检测到网络拥塞的时候拥塞窗口将停止增加，此时该算法进入第三阶段。在这一点上，首先把拥塞门槛设置成当前窗口尺寸（拥塞窗口和通告窗口中的最小值，但至少两个段）的一半，接着把拥塞窗口设置成一个最大尺寸的段，然后再使用这种慢启动技术重新启动。

由于实施了这样的拥挤控制方法，TCP有时被说成是自我定时的。这种拥挤控制算法工作得很好，因为发送方在分组丢失时很快地减少发送速率，从而阻止拥挤崩溃。

4. 一台路由器可以连接多少个网络？

解答：在理论上没有限值。在实践中，路由器厂商允许的物理接口数目往往限制可以连接的网络个数。但严格说来，也并非尽然，因为在某些情况下，在一个物理接口上也可以有不止一个网络。作为例子，当使用ATM或帧中继的永久虚电路的时候，每一个PVC可能都代表一个独立的第3层网络。

5. 在下列关于网络运行机制和所提供的服务的描述中，哪些语句适用于帧中继网络？（请选择你认为正确的字母序号）

（a）从本质上讲是电路交换的。

（b）保持用户信息和信令分离。

（c）采用LAPB规程。

（d）在链路层实现链路的复用和转接。

（e）提供面向连接的虚电路分组服务。
（f）采用简单的快速分组交换机。
（g）提供端到端的流控制和错误恢复功能。
（h）与X.25网络比较，具有较低的延迟和较高的吞吐率。
（i）是开展B-ISDN研究的主要技术成果。
（j）也称做信元中继。

解答：（b）（d）（e）（f）（h）

6. 一旦你的网络驱动软件的第2层协议成分接收到一个帧，它怎么知道该对这个帧做什么样的处理？

解答：大多数第2层协议都定义一个头，头中包括一个域，指示下一个高层协议。例如，以太网头包括一个叫做类型的域。如果该域的值是0800h，那么帧的数据部分（即第3层的分组）应该往上交给TCP/IP软件做进一步的处理。如果类型域的值是0806h，那么数据域的内容属于地址分辨协议（ARP）。

7．在下列几组协议中，哪一组属于网络层协议？

（a）IP和TCP
（b）ARP和TELNET
（c）FTP 和UDP
（d）ICMP和IP

解答：（d）

8. 数据是怎样递交给下一高层做进一步处理的？

解答：通常，当像是IP这样的一个协议在初始化的时候要为发送和接收分组建立若干个存储器缓冲区。当该协议被绑定到一个网络适配卡的时候，要为适配卡的设备驱动程序（即第2层软件）分配一个存储器地址，让它把从网络上接收到的数据放到那里。一旦适配卡驱动程序把数据放到指定的存储器地址，IP软件就可以开始处理这个来自下层的分组。

9．填空题

CCITT X.25 建议书定义了三级通信，即_____级、_____级和_____级。X.25建议书的第二级使用ISO的_____标准，主要目的是错误控制，称为_____方式。

解答：CCITT X.25 建议书定义了三级通信，即 物理 级、 链路 级和 分组 级。X.25 建议书的第二级使用ISO的 HDLC 标准，主要目的是错误控制，称为 链路访问协议平衡 方式。

10. 计算机A位于一个令牌环网络上，该令牌环网络通过一个路由器连接到一个以太网。这个以太网又用一个转换桥接器连接到另一个令牌环网络。计算机B驻留在第二个令牌环网络上。试说明对于由计算机A发给计算机B的数据会发生什么样的过程？

解答：在计算机A上的发送方应用程序把数据通过高层往下传递，直到它到达第3层，在那里它被放到一个网络层分组内部。然后，这个分组再被放到一个令牌环帧中。这个帧再被转变成电信号，并被放到网络线缆上传输。

因为第一个令牌环和以太网段是用一台路由器隔开的，而路由器工作在第3层，路由器必须丢弃令牌环帧的头部和尾部，然后读第3层分组的头。在确定了计算机B的位置之后，路由器在第3层分组上添加以太网的头部和尾部，形成一个新的以太网帧。接着，路由器发送以太网帧，把1和0转换成电信号（第1层）后再在线缆上传输。

一旦帧到达了工作在第2层的桥接器，桥接器确定计算机B驻留在第二个令牌环网段上。由于桥接器不关心也不懂得分组的内容（桥接器仅工作在第2层），但它知道所收到的以太网帧不能够在令牌环网上传输，桥接器必须剥除以太网帧的头部和尾部，再加上令牌环帧的头部和尾部（第2层），然后再发送这个帧。

11．填空题

帧中继是在_____网标准化过程中提出来的一种协议，它不采用LAPB规程，而是采用_____的一个子集，称为_____协议。

解答：帧中继是在_综合业务数据_网标准化过程中提出来的一种协议，它不采用LAPB规程，而是采用_LAPF_的一个子集， 称为_数据链路核心_协议。。

12．填空题

1988年，CCITT蓝皮书把ATM描绘成一种基于_____的交换技术。链路本身是全部基于光纤的点到点的干线，安排成每秒_____位范围内的等级速度。这些在美国称为_____网络的光纤链路与ATM交换机相耦合形成新一代的网络，就是宽带ISDN。

解答：1988年，CCITT蓝皮书把ATM描绘成一种基于_非通道化的高速数字链路_的交换技术。链路本身是全部基于光纤的点到点的干线，安排成每秒_千兆_位范围内的等级速度。这些在美国称为_SONET_网络的光纤链路与ATM交换机相耦合形成新一代的网络，就是宽带ISDN。

13. 既然ATM有一个第3层部件，为什么还需要在ATM上运行TCP/IP呢？

解答：事实上，不必要在ATM上运行TCP/IP。完全可以编写应用程序，直接请求ATM服务，使用20字节的ATM地址代替IP地址，允许ATM的路由选择通过互连的网络提供无回路的通路。实际上，ATM之所以这样有名望，就是因为它有这样的能力。但由于目前缺乏基于ATM开发的应用程序，且ATM实现的成本比较高，所以还不能够像以太网那样被普遍采用。

14．图5-1示出了四个连接在一起的ATM交换机，分别标记为A、B、C和D。在它们之间的粗白线表示光纤连接，点虚线表示PVC。在物理上，这是一个什么类型的拓扑？

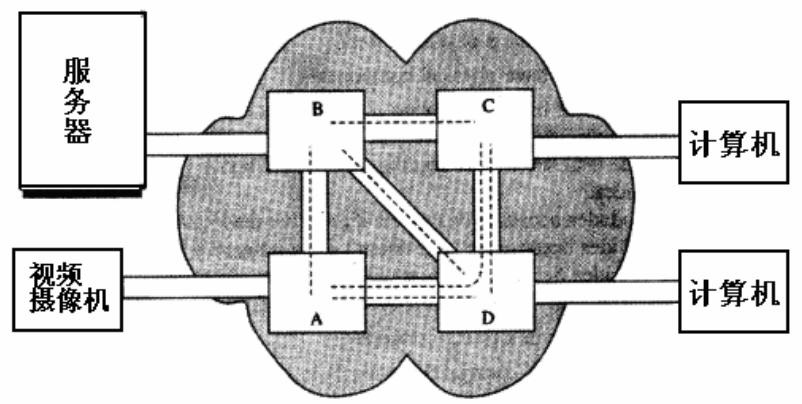


图 5-1　范例光纤网络

解答：在物理上，这是一个对等到对等网络的部分网状。如果把A和C交换机直接连接，那么这就会是一个完全网状。

15. 在逻辑上，图5-1所示的是什么类型的拓扑？

解答：在逻辑上，这是一个完全网状，因为所有交换机到所有其它交换机都通过一条PVC有直接连接。在交换机A和C之间没有物理连接的事实并不重要。

16. 在图5-1中，示出一条PVC从顶部PC到视频摄像机所有可能的通路。

解答：这些可能的通路是通过下列交换机：

- C，D，A
- C，B，A
- C，B，D，A
- C，D，B，A

从图中顶部PC到视频摄像机有4条可能的通路。无论是计算机还是摄像机都无法知道数据通过网络走什么样的通路。这种缺少可见性就是为什么ATM网络和其它基于虚电路的网络（例如帧中继）被称作“云”的原因。

使用这些连接的主要好处是可以为交通做路由选择，绕过拥塞的或断开的链路。例如，如果有一条SVC运载数据经过通路C、D、A，并且在交换机A和D之间的物理链路断开了，那么交通可以很快地被自动重新路由，取通路C、B、A。如果在B和C之间的链路遭受拥塞，使得ATM网络不能够保证维持恒定的位速率，那么该SVC可以选择通路C、D、B、A。虽然这种灵活性是非常宝贵的，但也带来了配制和排除故障都相当复杂的问题。

17. 假定一个单位有两个办公场点，想在每一个场点安装一台专用小交换机（PBX），让在一个场点的职员可以呼叫在另一个场点的职员，并且不用每个呼叫都向电话公司付费。该单位应该怎么做？

解答：从电话公司租用一条专用线路，例如T1线路或ISDN的PRI（基群速率接口）线路。然后把这条线路连接到每一个PBX。这将在两个办公场点之间允许最多可达23个同时

的电话会话。

虽然该单位确实需要有一条物理连接到达电话局，但T1（或ISDN-PRI）实际上是一个虚电路。不管它要经过多少个物理设备，但对两台PBX说来，它就像是一条导线。换句话说，如果两个办公室相隔好几个省，该电路把本地PBX连接到电话局的交换机，从那里再连接到其它电话局的交换机，也许要经过长途局，最后到达远程办公场点。然而所有这些看起来就像是连接PBX的单条链路。这是因为PSTN（公共交换电话网）是电路交换的。

18. 用一般的术语定义交换机的功能。

解答：交换机是用以执行交换功能的硬件，该功能包括在不同的网络和网段之间移动信息。

19. 选择题

端口映射器的作用是关联

（a）一个输出端口到媒体上一个可用的通道
（b）一个输入端口到一个输出端口
（c）一个输入端口到在交换机结构中的一个缓冲区
（d）在交换机结构中的一个缓冲区到一个输出缓冲区

解答：b. 一个输入端口到一个输出端口

端口映射器仅在分组交换机中使用，而不在线路交换机中使用。分组交换机包含一个把每个输入关联（映射）到一个输出的表。在输入端交换机读分组的目标地址，在表中找到它的位置，然后把一个输出端口分配给该分组。线路交换不需要端口映射器，因为当分组到达交换机的输入时，其前往目的地的输出已经为交换机所知。

20. 在中转交换机中减少阻塞是通过什么实现的？

（a）交换机使用不同输出的能力
（b）交换机使用不同输入的能力
（c）交换机使用不同纵横交叉元素的能力
（d）交换机预留输出的能力

解答：a. 交换机使用不同输出的能力

交换机具有使用不同输出的能力，因此能够减少阻塞的发生。

21. 什么是内部阻塞？

解答：当发生内部阻塞时，没有到达一个可提供的输出的通路。在缓冲区积累起来的等待同一输出的分组阻止排在更后面的其它分组前往它们的输出端口的机会。

22. 简要说明trie树的用途。

解答：可以使用不同的数据结构来执行较快的最好匹配查询。trie树就是一个常用的做最好匹配的数据结构。事实上，trie树是一种特别有用的索引结构。具体地讲，trie树的组织是一个数组的等级结构，其中每一项都可以取下列三个值中的一个：

- 如果在数据中的其它地方存在一个更好的匹配，该登记项将包含一个指向另一个数据的指针。
- 如果没有已知的更好匹配存在，该登记项将用一个特别的符号指明这个状态。
- 如果在树中该节点的父节点包含可能的有效数组，那么该登记项包含一个null指针。Null的作用是终结关键码。

当一个前往一个特别的目的地的分组到达时，假定前往同一目的地的其它分组还将到达。因此如果把从第一个分组的trie树函数得到的通路信息存放在快速缓冲区中，那么对于具有相同目的地地址的其它分组的通路可以在执行trie搜查之前先在缓冲区中检查。这样就可以改善trie树查询的性能。另一个假定是要查找的大多数地址是在本地设备的地址。因此如果把本地的地址放在trie等级结构中的较高位置，那么查找本地地址所需要的时间就会比较少。在实践中如果把上述两种技术一起使用，就可以大大提高交换机的性能。

23. 对于一个广播交换机需要有一个调度程序来安排交换操作吗？

解答：在广播机制中不需要调度程序，因为输入分组都被指定输出端口，而且是把分组广播到所有的输出端口。

24. 简要说明术语“交换结构（switch fabric）”的含义。

解答：交换结构是交换机的硬件和软件成分，它们把数据从一个交换机输入移到一个交换机输出。该结构的复杂度可以从只是把数据从输入端口拷贝、然后写到输出端口的简单技术，直到并行地把数以千计的分组传送到许多个输出端口的多处理机部件。

25. 电话交换机是下列交换机类型的一个范例：

a. 分组　　b. 缓冲　　c. 结构　　d. 线路

解答：d. 线路。线路交换的一个范例是电话交换机。线路交换处理在媒体上的分组，这些分组不包含任何元数据。

26. 为什么信元交换网络使用基于虚电路的交换而不使用基于数据报的分组交换？

解答：信元交换网络使用固定长度的分组，这导致对在传输媒体上的信号可进行预测分析，因此在传输数据阶段不需要使用网络设备的地址信息。使用虚电路交换的结果使得信元交换的运行效率更高，执行速度快，且易于管理。

27. 一个简单的纵横制交换机有8个输入线路和8个输出线路。在该交换机中有多少个交叉点？

解答：$8^2=64$

28. 什么是过度提供？

解答：过度提供是解决拥塞问题的方法之一。在过度提供机制中，在交换结构中的内部链路的执行速度比输入链路快。这种设计可以帮助竞争同一输出的到达分组在交换结构中可以被更快的内部链路运载。这种方法可以释放输入端口，并减少冲突。

29. 在X.25分组中，没有采用错误检测机制（无分组检查序列）。试说明为什么X.25还能保证所有传输的分组都被正确投递。

解答：尽管在X.25分组中，没有采用错误检测机制（无分组检查序列）,但在数据链路层采用HDLC或类似的协议，保证了端点设备跟X.25交换机之间以及X.25相邻交换机之间数据传送的完整性。另外，X.25分组格式设有发送和接收序列号，能够查出在结点转发过程中的分组丢失现象，并通过重置和重启动等措施加以恢复和纠正。所以，**X.25能够保证所有传输的分组都被正确投递**。

30. 在X.25的第2级和第3级都使用了流控机制。这样做多余吗？还是必需？试说明理由。

解答：在X.25的第2级和第3级都使用了流控机制。这样做是必需的。因为第2级使用的流控机制只能保证在端点设备跟X.25交换机之间以及在X.25相邻交换机之间数据传送的过程中不会发生溢出现象，而不能保证在从源端点设备到目的地端点设备数据传送的过程中不会发生溢出现象。所以，为了保证在从源端点设备到目的地端点设备数据传送的过程中不会发生溢出现象，第3级也必需使用流控机制。

31. 什么是分布式路径算法？

解答：分布式路径算法属于一种自适应路由选择算法，它让各相邻节点之间周期性或不定期地交换各自的时延表，并以此为基础重新产生各节点当时的新时延表和路由选择表。例如，节点C收到节点A、B和D的当前时延表，从其中可以分析出A、B、和D所属的各条数据链路的排队队列长度，这些队列相当于串接在节点C的各条路由中，因而可以据此重新算出节点C的新时延表和路由选择表。

32. 试述链路状态路由选择算法，在此路由选择算法中还使用了哪些其它的路由选择算法？

解答：“链路状态”(Link State)的算法也称作“最短路径优先”(Shortest Path First)，简称SPF。SPF算法要求每个参与协议的节点都有完全的网络拓扑信息，这里拓扑信息可以想象成每个节点都有一张地图，地图上标示了所有其它的节点以及它们所连接的链路。在抽象的术语中，路由器对应于图中的节点，而连接节点的链路对应于边。当且仅当对应的节点可以直接通信时，在这两个节点之间才有一条边(链路)。简言之，在一个链路状态路由选择协议中，一个节点检查所有直接链路的状态，并将所得的状态信息发送给网上所有其它的节点，而不是仅仅送给那些直接相连的节点。以这种方式，每个节点从网上所有其它的节点接收包含直接链路状态的路由选择信息。每当链路状态报文到达时，路由节点便使用这些状态信息去更新自己的网络拓扑和状态“视野图”，把各个链路标为“up”或“down”。一旦链路状态发生了变化，节点对更新了的网络图利用Dijkstra最短通路搜索算法重新计算路由。Dijkstra算法是从单一的报源出发计算到达所有目的节点的最短路径。

在此路由选择算法中，除了利用Dijkstra算法计算从单一的报源出发计算到达所有目的节点的最短路径外，还利用扩散法进行链路状态信息的分发。

33. 填空

形成网络中数据传输环路的原因是：_____、_____。解决的方法有是_____。

解答：形成网络中数据传输环路的原因是：___路由表错误___、___软件故障___。解决的方法有__设定生命期__。

34. 使用分布式路由算法绘制如图5-2所示的子网中B节点的路径表，请说明其绘制步骤。

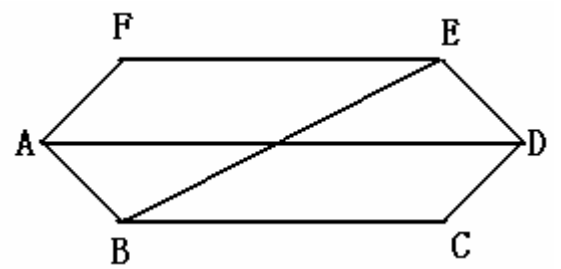


图 5-2　习题 33 插图

解答：绘制步骤：

（1）先在表中列出通过直接链路可到达的节点A、C和E。
（2）考虑B——>D, ∵BC+CD<BA+AD ∴下一节点取C。
（3）考虑B——>F,∵BA+AF<BE+EF　∴下一节点取A.

表5-1示出了B节点的路径表。

表5-1　B节点的路径表

目的节点	前往的下一邻居节点
A	A
C	C
E	E
D	C
F	A

35. 试述使用抑制分组策略实现拥塞控制的工作原理。

解答：每个路由器都监视其输出线路和其它资源的利用率。当一条输出线路的利用率超过临界值的时候，该输出线路就进入“警告”状态。路由器对新到达的每个分组都要检查它的输出线路是否处于警告状态。如果是，路由器就给该分组的源主机发送一个抑制分组，并在抑制分组中给出原分组的目的地。同时，路由器在原分组的头上做个标记（使用头中的某一位）表明对该分组已经发送过抑制分组，然后将该分组跟正常情况一样地继续沿通路向目的地转发。因此，其它路由器不会对该分组再产生抑制分组。当源主机收到抑制分组时，它被要求把发往指定目的地的交通量减少x%。由于可能又有若干前往同一目的

地的其它分组已经发出，并正在行进途中，从而可能产生更多的抑制分组，所以源主机应该在一个固定长度的时间内忽略跟该目的地有关的其它抑制分组。在那段时间之后，源主机在另一个固定长度的时间内侦听是否又有抑制分组到达。如果有一个抑制分组到达，说明线路仍然拥塞，因此源主机更多地减少数据流，并开始再次忽略跟该目的地有关的其它抑制分组。如果在侦听时间段内没有抑制分组到达，主机可以再增加数据流。

这种明确的反馈机制可以帮助防止拥塞，但不压制通过的数据流。主机可以根据它的策略参数来减少交通，例如调节窗口大小或漏桶输出速率。典型地，第一个抑制分组使得数据速率减少到原来速率的0.50，下一个抑制分组使得减少到原来速率的0.25，等。流量增加的速度宜以小的增量逐步进行，以防止很快又再次发生拥塞。

36.填空

用于拥塞控制的漏桶算法中有3个重要参数：

C-桶内的数据量，Bc-许诺的突发量，Be-附加的突发量。

当C在Bc与Bc+ Be之间时，桶内的数据量减少_____。否则，若桶内的C不是负值，且小于或等于Bc，那么，数据转发时，桶内数据量减少的值应为_____（见提示）。

提示：a. C或Bc

b. Max[C, Bc]

c. Min[C, Bc]

解答：C-桶内的数据量，Bc-许诺的突发量，Be-附加的突发量。

当C在Bc与Bc+ Be之间时，桶内的数据量减少__C__。否则，若桶内的C不是负值，且小于或等于Bc，那么，数据转发时，桶内数据量减少的值应为_c. Min[C, Bc]_。

5.3 综合应用练习题

1. 遵从ANSI帧中继封装标准，使用帧中继在1.544Mbps的T1链路上最多可复用多少条连接？

解答：DLCI（数据链路连接标识符）段是10位，这就意味着在链路上虚电路的总数是2^{10}即1024。答案跟链路的速度或类型无关。其它厂商使用专用的格式，可以有更多的虚电路。另外，如果想增加虚电路的数目，还可以使用地址扩展段在头中加入第2个字节。

2. 在帧中继网络上，当一个BECN位置1的帧到达时，接收设备会作出什么样的举动？

答：在理论上，该设备会减少它的发送速率，直到收到的帧不再把BECN位置1为止。然而，这一举动是可选的，大多数的帧中继设备厂商允许管理员决定是否对BECN作出响应。

3. 如果ISDN是交换的，那么它是如何把数据从网络上的一点传到另一点的呢？

解答：ISDN是在一个复杂的设备系列中实现的。设备用标记参照点的接口连接。从承

载网络开始，ISDN交换机通过U接口连接到NT1（网络终端设备1）。NT1再通过T接口连接到NT2（网络终端设备2）。NT2再使用S参照点连接到一个数据终端（TE1）或一部ISDN电话（TE1）。从用户终端出发，连接顺序是：数据终端—>S参照点—>NT2—>T接口—>NT1—>U接口—>ISDN交换机。就一个企业而言，载体部门典型地是把一个网络端接设备NT1放在客户的室内，NT1跟载体部门的ISDN交换机之间的距离一般有几公里，使用通常用于模拟电话的由两根铜导线构成的双绞线互连。设备NT2一般是一个PBX（专用小交换机），通过一对双绞线即4线的数字链路连接到NT1。参照点S则是在ISDN PBX和ISDN终端之间的接口，提供对电话、终端和其它设备的连接。

ISDN也像电话网那样使用地址。在基本速率接口（BRI）上每个B通道得到一个SPID，标识跟ISDN交换机的接口。对这个接口进行配制就可以实现拨号功能，所拨的号码被用来通过ISDN网络对数据做路由选择。有了路由选择功能，就可以把数据从网络上的一点传到另一点。

4. ISDN是怎样能够同时支持话音和数据服务的？

答：ISDN B通道是64kbps，刚好是脉冲编码调制（PCM）所需要的大小。这种把模拟话音信号转换成二进制1和0的流的非常简单且低时延的方法允许单个呼叫占据单个通道。

因为ISDN是数字的，分组化的数据交通也容易通过网络传输。而且，因为每个通道具有固定的带宽，通道之间互不干扰，因此来自一个通道的数据不会延迟在另一个通道上的数据或话音。

5. 对于图5-3中所给出的网络，试列出到达每一个目的地节点的数据报转发表。图中对每条链路都已标出了相对代价；你的转发表应该能够把每个分组都通过最小代价通路往目的地转发。

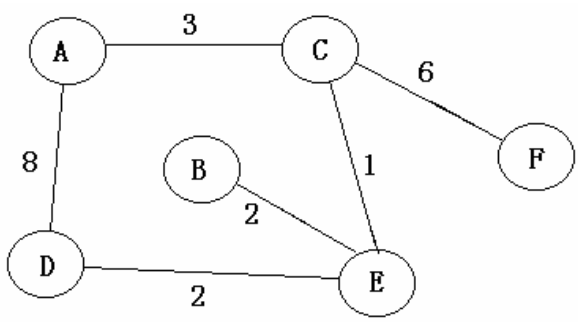


图 5-3　习题 5 插图

解答：

节点A

目的地	下一跳段
B	C
C	C
D	C
E	C
F	C

节点B

目的地	下一跳段
A	E
C	E
D	E
E	E
F	E

节点C

目的地	下一跳段
A	A
B	E
D	E
E	E
F	F

节点D

目的地	下一跳段
A	E
B	E
C	E
E	E
F	E

节点E

目的地	下一跳段
A	C
B	B
C	C
D	D
F	C

节点F

目的地	下一跳段
A	C
B	C
C	C
D	C
E	C

6. 图5-4中每个圆圈代表一个网络节点，每一条线代表一条通信线路，线上的标注表示两个相邻节点之间的代价。请根据Dijkstra最短通路搜索算法找出A到F的最短路径。要求在答案中（1）表示出从A到F的最短路径（2）给出从A到F的这个最短路径的代价

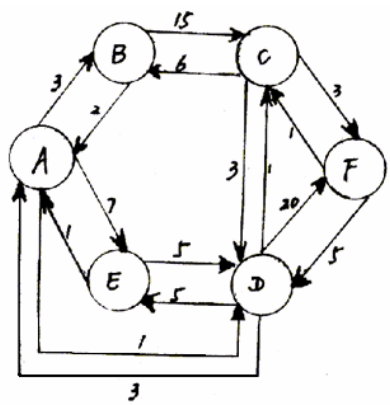


图 5-4　习题 6 插图

解答：（1）

A→ D → C → F

（2） 5

7. 图5-5中每个圆圈代表一个网络节点，每一条线代表一条通信线路，线上的标注表示两个相邻节点之间的代价。

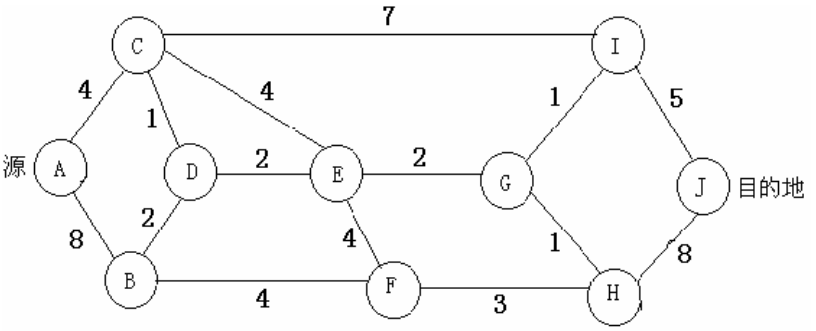


图 5-5　习题 7 插图

请根据Dijkstra最短通路搜索算法找出A到J的最短路径。规定使用直接在图上加标注的方法，而且，在答案中只要求：

（1）依次列出每一步的工作节点

（2）给出从A到J的最短路径及代价

（3）在原图上示出最后一步算法完成时图上每个节点（除A以外）的标注。

解答：（1）每一步的工作节点如下：

ACDBE（或EB）GIH（或HI）FJ。

（2）从A到J的最短路径是A→C→D→E→G→I→J ，代价等于 15。

（3）最后一步算法完成时图上每个节点（除A以外）的标注如图5-6所示。

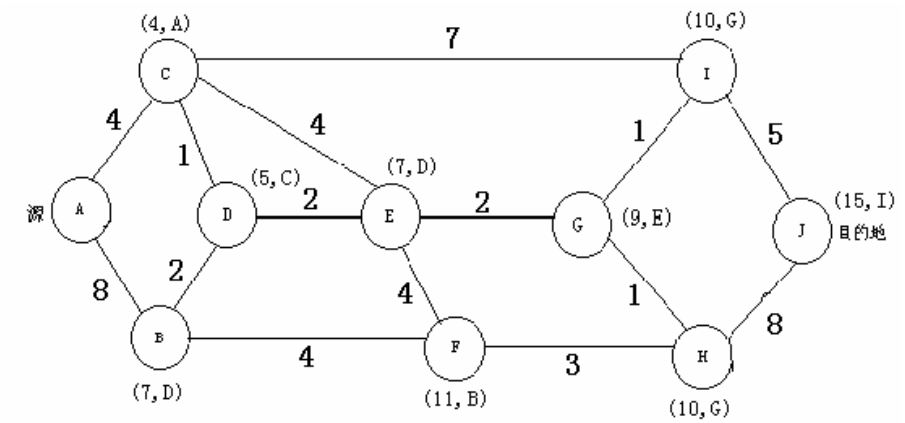


图 5-6　最后一步算法完成时图上每个节点（除 A 以外）的标注

8. 有5个路由器要连成一个点到点结构的子网。在每一对路由器之间可以设置一条高速线路，或者是一条中速线路，或者是一条低速线路，也可以不设置任何线路。如果产生和考察每一种拓扑要化100ns的计算机时间，那么，为了寻找匹配预期负载的拓扑而考察所

有可能的拓扑需用多长时间？

解答：设这5个路由器分别叫做A、B、C、D 和E。存在10条可能的线路：AB，AC，AD，AE，BC，BD，BE，CD，CE和DE。它们中的每一条都有4种可能性：3种速率以及没有线路；因此总的拓扑数是4^{10}=1048576。因为每种拓扑化100毫秒的时间，所以，总共需用的时间为104857.6秒，约等于29小时。

9. 2^n-1个路由器互相连接成一个集中式二叉树，树的每个节点上都有一个路由器。路由器i要和路由器j通信，必须先把信息发到树的根，然后根再把信息往下发给j。假定每一对路由器间的通信都类似，请推导出在n取值很大的条件下每个信息传输所经过的平均跳段数的近似表达式。

解答：路由器到路由器通路的平均长度是路由器到根的通路的平均长度的2倍。设根在树中的层号是1，最深的层号是n。显然，总的节点数等于

$N=1+2+4+\ldots+2^{n-1}=1\times(2^n-1)\div(2-1)=2^n-1$

从根到第n层的通路需要n-1跳段，第n层路由器的数目是2^{n-1}，当n很大时，

$2^{n-1}\div N\approx 2^{n-1}\div 2^n=1/2$，即有一半的路由器位于第n层。

从根到第n-1层的通路要n-2跳段，第n-1层路由器的数目是2^{n-2}，当n很大时，

$2^{n-2}\div N=2^{n-2}\div(2^n-1)\approx 2^{n-2}\div 2^n=1/4$，

因此，平均通路长度为：

$L=0.5\times(n-1)+0.25\times(n-2)+0.125\times(n-3)+\ldots+0.5^{n-1}\times[n-(n-1)]+0.5^n\times(n-n)$

$=0.5n+0.25n+0.125n+\ldots+0.5^n\times n-[0.5\times 1+0.5^2\times 2+0.5^3\times 3+\ldots+0.5^n\times n]$

$=(0.5+0.25+0.125+\ldots+0.5^n)\times n-(1+0.5+0.25+\ldots+0.5^n\times 2)=1\times n-2=n-2$

$2L=2n-4$

所以，路由器到路由器通信的平均跳段数近似为2n-4。

10．为什么ATM使用小的固定长度的信元？

解答：小的定长信元可以快速地选择路径通过交换机，并且对其进行的交换操作可以完全用硬件来实现。

11．给出两个适合于使用面向连接的服务的示例应用。再给出两个最好使用无连接服务的例子。

解答：文件传送、远程登录和视频点播需要面向连接的服务。在另一方面，信用卡验证和其它的销售点终端、电子资金转移，以及许多形式的远程数据库访问生来具有无连接的性质，在一个方向上传送查询，在另一个方向上返回应答。

12．有没有虚电路服务需要以非顺序的方式投递分组的情况？请解释。

解答：有。中断信号应该跳过在它前面的数据，进行不遵从顺序的投递。典型的例子是当一个终端用户键入退出（或kill）键时。由退出信号产生的分组应该立即发送，并且应该跳过当前队列中排在前面等待程序处理的任何数据（即已经键入但尚未被程序读取的数据）。

13．数据报网络把每个分组都作为独立的单元（独立于所有其它单元）进行路由选择。虚电路网络则不必这样做，每个数据分组都遵循一个事先确定好的路由。这个事实意味着虚电路网络不需要从任意源到任意目的地为分组做路由选择的能力吗？

解答：不对。为了从任意源到任意目的地为连接建立分组选择路由，虚电路网络肯定需要这一能力。

14．给出连接建立时可能要协商的协议参数的3个例子。

解答：在连接建立时可能要协商窗口大小、最大分组尺寸和超时值。

15．考虑下列关于实现虚电路服务的设计问题。如果在内部网络中使用虚电路，每个数据分组必须有一个3字节的头，每个路由器必须固定分配8个字节的存储器用于电路标识。如果在内部网络中使用数据报，需要用15字节的头，但不需要路由器的表空间。每跳段传输容量的代价是每10^6字节1分钱。路由器的存储器的购价是每字节1分钱，使用期限为2年的工作日。统计的平均会话运行1000秒，在此期间传送200个分组，平均1个分组需要传输4个跳段。哪一种实现要便宜一些？便宜多少？

解答：4个跳段意味着涉及5个路由器。虚电路实现需要在1000秒内固定分配5×8=40字节的存储器。数据报实现需要比虚电路实现多传送的头信息的容量等于（15-3）×4×200=9600字节-跳段。现在的问题就成了40000字节-秒的存储器对比9600字节-跳段的电路容量。如果存储器的使用期是两年，即$3600\times8\times5\times52\times2\approx1.5\times10^7$秒，1个字节-秒的代价为$1\div(1.5\times10^7)=6.7\times10^{-8}$分，那么40000字节-秒的代价约等于2.7毫分。另一方面，1个字节-跳段代价是10^{-6}分，9600个字节-跳段的代价为$10^{-6}\times9600=9.6\times10^{-3}$分，即9.6毫分。显然，对于这样的参数，虚电路的实现要便宜一些。9.6-2.7=6.9毫分，即在这1000秒的时间内便宜大约6.9毫分。

16．假定所有的路由器和主机都工作正常，所有软件的运行也都没有错误，那么是否还有可能（尽管可能性很小）会把分组投递到错误的目的地？

解答：有可能。大的突发噪音可能破坏分组。使用k位的检验和，差错仍然有2^{-k}的概率被漏检。如果分组的目的地段或虚电路号码被改变，分组将会被投递到错误的目的地，并可能被接收为正确的分组。换句话说，偶然的突发噪音可能把送往一个目的地的完全合法的分组改变成送往另一个目的地的也是完全合法的分组。

17．请给出一个简单的试探方法，寻找通过一个网络从一个给定的源到一个给定的目的地的两条通路（假定确实存在两条这样的通路），以便在任一条通信线路失效的情况下，在这两个节点之间还能进行通信。假定路由器是足够可靠的，因此不必担心路由器崩溃的可能性。

解答：使用最短通路搜索算法选择一条路径，然后，删除刚找到的路径中使用的所有的弧（对应一条条链路）。接着，再运行一次最短通路搜索算法。这个第2条路径在第1条路径中有线路失效的情况下，可以作为替代路径启用；反之亦然。

18. 考虑在图5-7中示出的网络，忽略在线路上的权值。假定它使用洪泛作为路由算法。

如果一个由A发往D的分组有最大跳段计数3，试列出它将采取的所有路径。同时说明它消耗了多少个跳段的带宽。

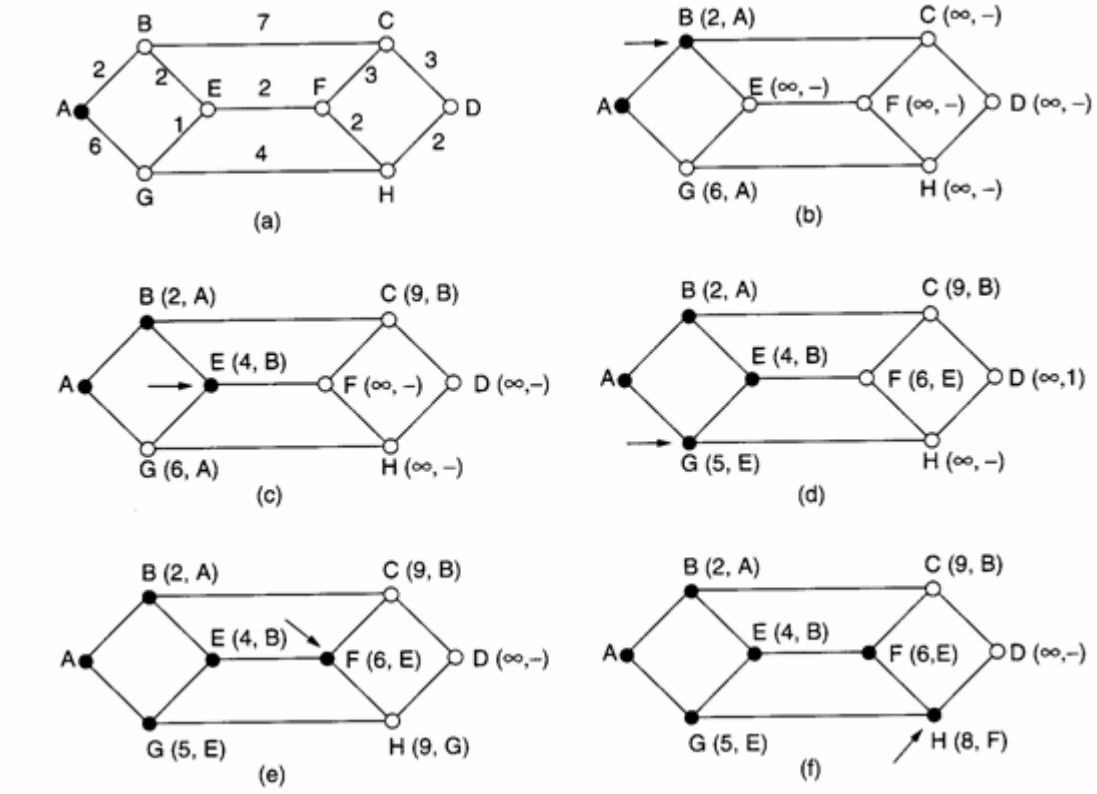


图 5-7　在计算从 A 到 D 最短通路过程中的前 5 步，箭头表示工作节点

解答：洪泛分组经过了下列路径：ABCD,ABCF,ABEF,ABEG,AGHD,AGHF,AGEB和AGEF。使用的跳段数是24。

19. 考虑在图5-8(a)中示出的网络。假定在F和G之间加入一条新的线路，但图5-8(b)的沉落树保持不变，图5-8（c）会有什么样的改变？

解答：节点F原来有两个子节点A和D，它现在又有了第3个子节点G,它没有加圈，因为遵从路径IFG的分组不在沉落树上。节点G除了有D作为其子节点，又有了第2个子节点F。F也没有加圈，因为它也不在沉落树上。

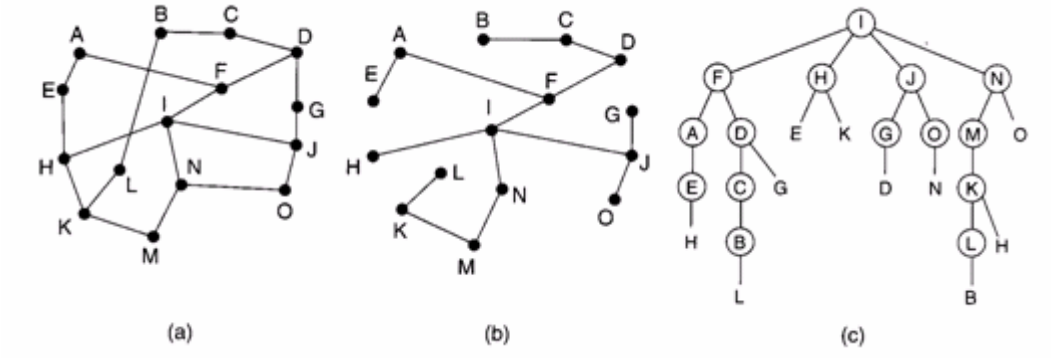


图 5-8　反向通路　　(a)子网　　(b)沉落树　　(c)通过反向通路转发建立的树

20. 在图5-9示出的起始于A的查询中，节点H或I也会广播分组吗？

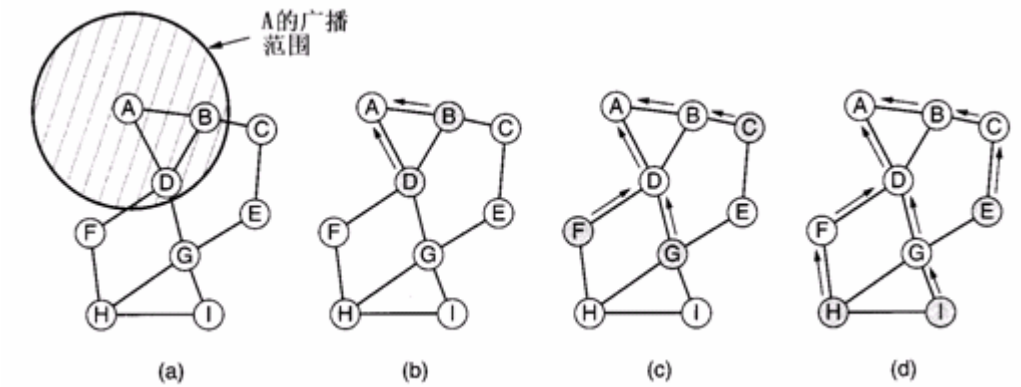


图 5-9 (a)　A 的广播范围；　　(b) 在 B 和 D 接收 A 的广播之后；
(c) C、F 和 G 接收 A 的广播之后；　　(d) E、H 和 I 接收 A 的广播之后。
阴影节点是新的接收者，箭头表示可能的反向路径。

解答：当H得到分组时，它会广播。然而，I节点知道如何到达I，因此它不会广播。

21. 假定在图5-9中的节点B刚刚重新引导，在其表中没有路由信息。它突然需要前往H的路由，它发出广播，并把TTL设置成1，2，3等。它要用多少轮才能找到一条路由？

解答：节点H离B有3个跳段，因此它需要用3轮才能找到路由。

22. 作为在对等网络中节点查询的一种算法，chord算法是怎样工作的？

解答：对等（peer-to-peer）系统完全是分布式的。所有的节点都是对称的，没有中心控制或层次。在典型的对等系统中，用户都有一些其他用户可能对其感兴趣的信息，这些信息可能是自由软件、音乐、相片等。如果有大量用户，那么，彼此可能不熟悉，不知道到哪里可以找到它们所需要的信息。因此问题在于，在没有中心数据库甚至没有集中索引的情况下，一个用户怎样能够找到含有他寻找的信息的节点？

我们假定，每个用户都有1个或多个像是歌曲、相片、程序、文件这样的数据项目，并

且允许其他用户阅读。每个数据项用一个ASCII串命名，一个潜在的用户只知道这个ASCII串，并且想知道是否有其他人具有这个拷贝，如果有，他们的IP地址是什么。

解决问题的一种算法称作chord算法。Chord系统由n个参与的用户构成，每个用户都可能存有一些记录，每个记录都备有索引供其他用户使用。每个用户节点都有一个IP地址，该地址被通过一个散列函数转化成一个m位的数字。Chord使用SHA-1作为散列函数，该散列函数取一个可变长度的字节串，产生一个高度随机的160比特数字。因此，我们可以把任一IP地址转化成一个160比特的数字，称作节点标识符。

在概念上，可以有2^{160}个节点标识符，我们把它们以升序的方式安排在一个大的圆周上。在它们当中，有一些对应着实际的节点，但大多数都不是。在图5-10(a)中，我们示出m=5的节点标识符圆周。在这个例子中，具有标识符1、4、7、12、15、20和27的节点对应实际的节点，其它都不存在。

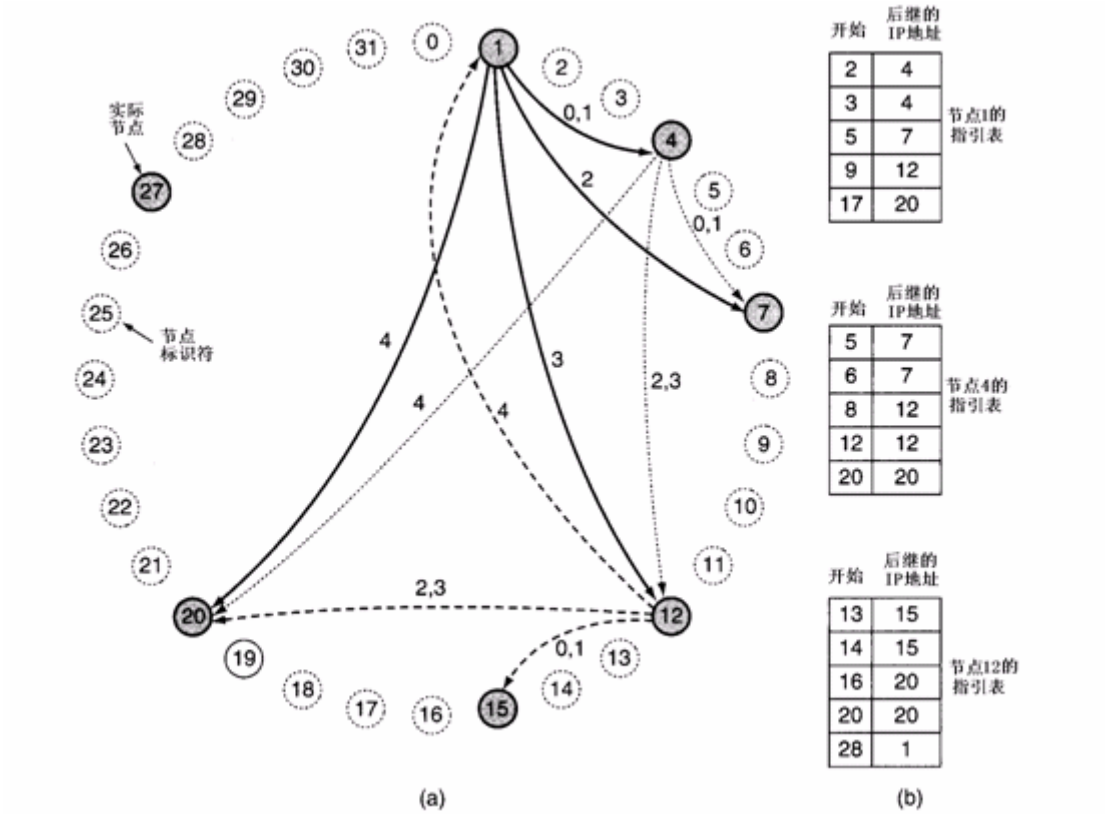


图 5-10(a)一组安排在一个圆周上的 32 个节点标识符。阴影节点对应实际的机器，弧表示从节点 1、4 和 12 得到的指纹。在弧上的标记是表索引 （b）指纹表范例

我们把函数successor(k)定义为在圆周上沿顺时针方向后随k的第1个实际节点。例如，successor(6)=7，successor(8)=12，successor(22)=27。

记录名（歌名等）也使用散列函数（例如SHA-1）生成一个160比特的数字，称作关键字。这样，我们可以使用key=hash(name)把记录的ASCII名字转换成它的关键字。这种计算只是一个对hash函数的本地过程调用。如果一个持有名字为name的歌曲记录的人想把该记

录提供给每个人使用，他首先建立一个由（name, my-IP-address）构成的数组，然后请求successor(hash(name))存储该数组。如果在不同节点上存在着多个以这个名字命名的记录，它们的数组将被存放在同一节点。这样，索引就被随机地分布在节点上。

如果某个用户随后要查找name，他就把name散列，产生关键字，接着使用successor(key)寻找存放其索引数组的节点的IP地址。上述第1步是容易的，第2步就不容易了。为了使得寻找对应某个key的节点的IP地址成为可能，每个节点必须维持一些管理数据结构。其中之一就是沿着节点标识符圆周它的后续节点的IP地址。例如在图5-10中，节点4的后继是7，节点7的后继是12。

现在我们就可以这样进行搜索。请求节点给它的后继节点发送一个包含自己的IP地址和要查询的key的分组。该分组围绕着环传播，直到它找到所查询的节点标识符的后继位置。那个节点检查它是否有匹配该key的信息，如果有，就把它直接返回给请求节点。

作为第一个优化，每个节点可以保存其后继和前驱的IP地址。查询可以顺时针或反时针发送，主要取决于哪条通路更短一些。例如，在图5-10中节点7可以沿顺时针找到节点标识符10，可以沿反时针找到节点3。

尽管有方向的两个选择，线性地搜索所有的节点在大的对等系统中是非常低效的。为了进一步地加速搜索过程，每个节点还维持一个指引表。该指引表有m个登录项，以0到m-1搜索，其中的每一个登录项都指向一个不同的实际节点。每个登录项有两个域：起点（start）和对应successor（start）的IP地址,如图5-10（b）所示。

在节点k，登录项i的域值是：

Start = $k+2^i$(modulo 2^m)

Successor(start[i])的IP地址。

在这里，每个节点存储相对少量节点的IP地址。

使用指引表，在节点k的对key的查询可以用下列公式进行。如果key落在k和successor（key）之间，那么持有关于key的信息的节点就是successor（k），搜索终止。否则，搜索指引表找出其start是最接近key的前驱的登录项。然后把一个请求直接发往在那个指引表登录项中的IP地址，请求它继续搜索。由于它比较接近key，但仍在key值之下，所以很有可能只用少量的附加查询就可以返回答案。事实上，每次查询都把到目标的距离减半，平均查询次数是log2n, n是实际的节点总数。

作为第一个例子，考虑在节点1上查询key=3。由于节点1知道3位于在它自己跟其后继4之间，所需要寻找的节点是4，因此查询终止，返回4的IP地址。

作为第二个例子，考虑在节点1上查询key=14。由于14不在1和4之间，需要查询指引表。离14最近的前驱是9，因此，请求被转发到指引表中对应登录项9的IP地址，即节点12的IP地址。节点12发现14在它自己和它的后继（15）之间，因此它返回节点15的IP地址。

作为第三个例子，考虑在节点1上查询key=16。这里也需要查询指引表，16的最近的前驱是9，请求被转发到登录项9的IP地址，即节点12的IP地址，但节点12自己不知道答案，它查询离16最近的前驱，找到14，由此产生节点15的IP地址。查询被发往节点15。节点15注意到16位于它和其后继（20）之间，因此它返回20的IP地址。

23. 考虑在图5-10中的chord圆周。假定节点10突然作为实际节点连进对等网络，这会

影响节点的指引表吗？如果回答是肯定的，那么会有什么样的影响？

解答：会影响节点的指引表。在排序为第3的登录项（不是序列号0，也不是1-2和4）中的节点由12改为10（参见插图5-11）。

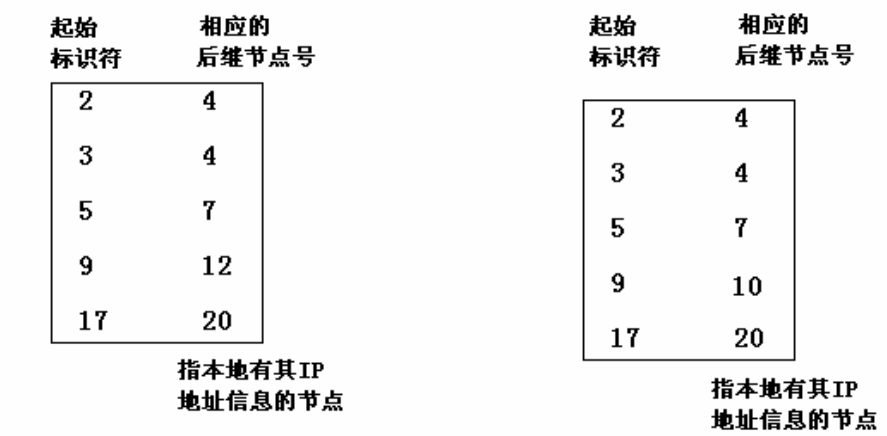


图 5-11　习题 20 插图

24. 在chord算法（关于对等查询）的简单版本中，搜索不使用指引（finger）表。在圆周的每个方向上搜索都是线性的。一个节点能够精确地预知应该在哪个方向上搜索吗？

请讨论你的答案。

解答：它可以近似地预测，但做不到精确。假定有1024个节点标识符。如果节点300要查找800，也许它最好是顺时针查找，但也可能在顺时针方向上在300和800之间有20个实际节点，而在逆时针方向上在它们之间仅有16个实际节点。加密散列函数SHA-1的目的是产生一个非常平滑的分布，使得沿着圆周的节点密度大约相同。但是总会有统计式波动，因此直接的选择可能是错误的。

25. 什么是ad hoc无线网络？

解答：Ad hoc无线网络是一个有两个或更多个具有无线通信和网络连接能力的设备的集合。这些设备都可以跟在它们的无线范围内的另一个节点直接通信，或者也可以跟它们的无线范围之外的节点通信。在后者的情况下使用一个中间节点把分组从源向着目的地中继或转发。

Ad hoc网络是自组织的和自适应的。这就意味着所形成的网络可以动态地重构而不需要任何系统管理。术语“Ad hoc”意味着“可以取不同的形式”，并且“可以是移动的、独立的或连网的”。Ad hoc节点或设备应该能够检测到其它同类设备的存在，并执行必要的握手过程，以便允许通信和共享信息和服务。

由于Ad hoc无线设备可以取不同的形式，例如掌上电脑、笔记本和因特网电话等，设备的计算、存储和通信能力可能差别很大。Ad hoc设备应该不但能够发现跟邻接设备或节点的连接性的存在，而且能够识别这些设备的类型以及它们对应的属性。由于一个Ad hoc无线网络不依赖任何固定的网络实体，它本身基本上就是一个无基础的网络。不必有固定

的基站，没有导线，也没有固定的路由器。然而，由于存在移动性，必须交换路由信息以反映链路连接性的变化。

Ad hoc移动设备的多样性还意味着它们的电池容量的差别。由于Ad hoc网络的节点需要对由其它节点发送的数据分组进行转发，功耗就成了关键的问题。

26. 传统网络的路由选择与无线ad hoc网络中的路由选择之间的主要差别是什么？

解答：基于最短通路的路由选择不适合无线ad hoc网络。在时间T计算的最短ad hoc路由在时间T+1可能不再有效，因为在路径上的任何节点都可能已经移动了，或者在路径上的链路特征可能已经改变。因此需要有一个新的路由选择方法。

传统的路由度量关注的特征是：

- 对于链路变化的快速自适应（指路由恢复时间）；
- 到目的地的最小跳段数通路；
- 传播延迟；
- 避免回路；
- 链路容量。

然而，在无线ad hoc网络中，以频繁的广播和过量的无线带宽消耗为代价的快速自适应是不可取的。好的路由质量不应该包括跳段数目和往返路程传播的时延。

由于具有较小跳段数值但有效期短的路由因频繁的数据流中断和需要做频繁的路由重构而效果很差，在ad hoc移动网络中路由长活性是最重要的。这种新的度量理念表明，经典的最短通路度量既不必用于也不可用于ad hoc无线网络。从另一个角度看问题，公平路由中继负载也是重要的，因为没有一个特别的移动节点应该不公平地承担支持许多条路由和执行许多分组中继功能的任务。这是一个公平性的问题，均匀路由中继负载可以减少在ad hoc移动网络中发生拥塞的可能性。

27. 按需距离向量（AODV）算法与常规的距离向量算法的不同点是什么？

解答：AODV（Ad hoc On-Demand Distance Vector）算法不是像常规的距离向量算法那样维持整个路由表，而是在按需的基础上建立路由，从而减少所需要的广播数目。AODV是一个按需获得路由的系统，因为不在所选通路上的节点不用维持相关的路由信息，不参与相关的路由表交换。

28. 什么是基于关联的长活路由选择（ABR）？它由哪三个阶段构成？

解答：ABR（Associativity-Based Long-lived Routing）协议是由源起始的按需路由协议，它由三个阶段构成：

- 路由发现阶段；
- 路由重构阶段；
- 路由删除阶段。

开始，当源节点需要一条路由时，调用路由发现阶段。当由于源/目的地/中间节点或子网-桥接移动主机迁移引起所建立的路径的链路改变时，调用路由重构阶段。当源节点不再

需要该路由时，它发起路由删除阶段。

29．考虑图5-12所示的子网。使用距离向量路由选择，下列向量刚刚被路由器C收到：

来自B：（5，0，8，12，6，2）
来自D：（16，12，6，0，9，10）
来自E：（7，6，3，9，0，4）

路由器C测量得到的到达B、D和E的延时分别等于6、3和5。试问路由器C的新的路由表是什么？请给出所使用的输出线路和所预期的延时。

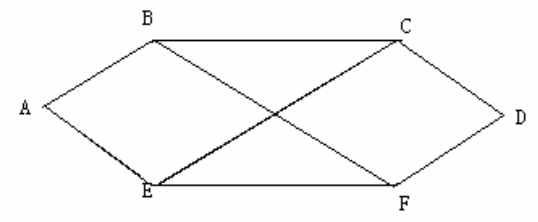


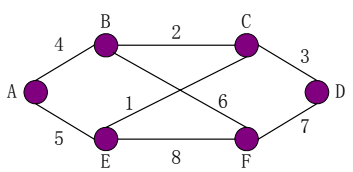
图 5-12　习题 29 插图

解答：　通过B给出　（11，6，14，18，12，8）
通过D给出　（19，15，9，3，12，13）
通过E给出　（12，11，8，14，5，9）
取到达每一目的地的最小值（C除外）得到：
（11，6，0，3，5，8）
输出线路是：（B，B，-，D，E，B）

30．在一个有50个路由器的网络中，假定延时用8个比特记录，每个路由器有3条线路跟其它路由器互连，每秒钟交换两次延迟向量。试问，该分布式路由器算法在每条线路上（全双工）消耗了多少带宽？

解答：路由表的长度等于8×50=400比特。该表每秒钟在每条线路上发送2次，因此，400×2=800bps，即在每条线路的每个方向上消耗的带宽都是800bps。

31．图5-13(a)给出了一个示例子网，其延时已标在线路上，图5-13(b)示出了所有六个路由器的对应的链路状态分组。



（a）子网

A	
序号	
存活时间	
B	4
E	5

B	
序号	
存活时间	
A	4
C	2
F	6

C	
序号	
存活时间	
B	2
D	3
E	1

D	
序号	
存活时间	
C	3
F	7

E	
序号	
存活时间	
A	5
C	1
F	8

F	
序号	
存活时间	
B	6
D	7
E	8

（b）该子网的链路状态分组

图 5-13　链路状态分组

源	序列号	存活时间	发送标志			ACK 标志			数据
			A	C	F	A	C	F	
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

图 5-14　在图 5-13 中的路由器 B 的分组缓冲区

在图5-13(a)所示子网中，路由器B所用的数据结构如图5-14所示。这里的每一行对应一个新近到达的但尚未完全处理完的链路状态分组。这张表记录了分组来自何处，它的顺序号、存活时间以及数据。另外，对于B的三条线路(分别前往A、C和F)中的每一条都有发送和应答标志。发送标志表示该分组必须在所示线路上发出去。应答标志表示该分组必须在那儿应答。

在图5-14中在每一行上的两组ACF比特的布尔“或”都是111。这只是一种巧合，还是对所有的子网在所有的情况下都成立？

解答：这个结论总是成立的。图5-14示出的是路由器B所使用的数据结构，A、C和F是它的三个相邻节点。如果一个分组在一条线路上到达，则必须在该线路上返回对它的确认。如果该分组没有从某一条线路上接收过，那么，它必须在该线路上转发。

32．对于具有4800个路由器的等级式路由，为了尽量减少三级结构的路由表的尺寸，区（REGION）和簇（CLUSTER）的大小应当如何选择？

解答：当使用等级式路由时，把整个网络内的路由器按区（REGION）进行划分，每个路由器只须知道在自己的区内如何为分组选择路由到达目的地的细节，而不用知道其它区的内部结构。对于大的网络，也许两级结构是不够的，还可以把区组合成簇（CLUSTER），把簇再组合成域（ZONE），…。对于等级式路由，在路由表中对应所有的本地路由器都有一个登录项，所有其它的区（本簇内）、簇（本域内）和域都缩减为单个路由器，因此减少了路由表的尺寸。在本题中，4800=15×16×20。当选择15个簇、16个区，每个区20个路由器时（或等效形式，例如20个蔟、16个区，每个区15个路由器），路由表尺寸最小，此时的路由表尺寸为15+16+20=51。

33．如图5-15所示，从所有的源（参见图a）到一个给定的目的地的最佳路由的集合形成一个沉落树（参见图b）。试问，从B做广播要产生多少个分组？

（a）反向通路转发　（b）沉落树

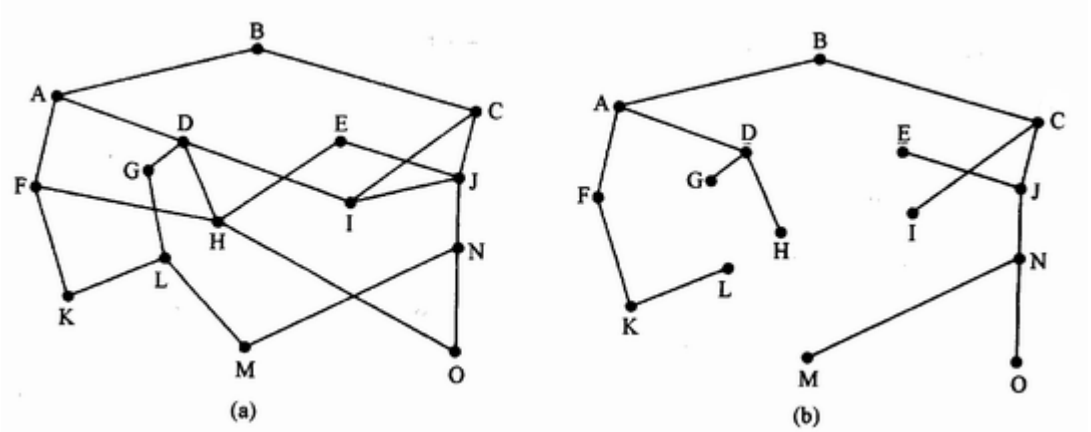


图 5-15　习题 33 插图　（a）一个子网　（b）路由器 B 的沉落树

解答：在一个子网中，从所有的源到一个指定的目的地的最佳路由的集合形成一棵以该目的地为根的树。这样的树就称作沉落树。沉落树不必是唯一的，其它具有相同通路长度的树可能存在。所有路由选择算法的目标都是要为所有的路由器寻找和使用沉落树。在广播形式的应用中，源主机需要向所有其它的主机发送报文。在称为反向通路转发的广播路由选择中，当广播分组到达路由器时，路由器对此分组进行检查，查看该分组是否来自于通常用于发送分组到广播源的线路，如果是，则此广播分组本身非常有可能是从源路由器来的第一个拷贝。在这种情况下，路由器将此分组复制转发到进入线路以外的所有线路。然而，如果广播分组到来的线路不是到达源端的线路，那么分组就被当作副本而扔掉。

（a）反向通路转发算法产生的树如图5-16所示。在第一站点，B发送分组到A和C（产生2个分组），如树中第二行所示。每个分组都在前往B的所选通路上到达（假定所选的通路沿着沉落树），并且用带圆圈的字母表示所到达的路由器。在第2跳段中，产生4个分组，在第1跳段中收到1个分组的每个路由器都产生两个分组。这4个分组都到达先前未访问过的路由器，并且都在前往B的所选通路上到达。在第3跳段所产生的10个分组中，仅5个是在前往B的所选通路上到达（K，G，H，E和N），并且仅这些分组所到达的路由器进一步产生分组。如此继续下去，算法进行到5个跳段后结束，总共产生28个分组。

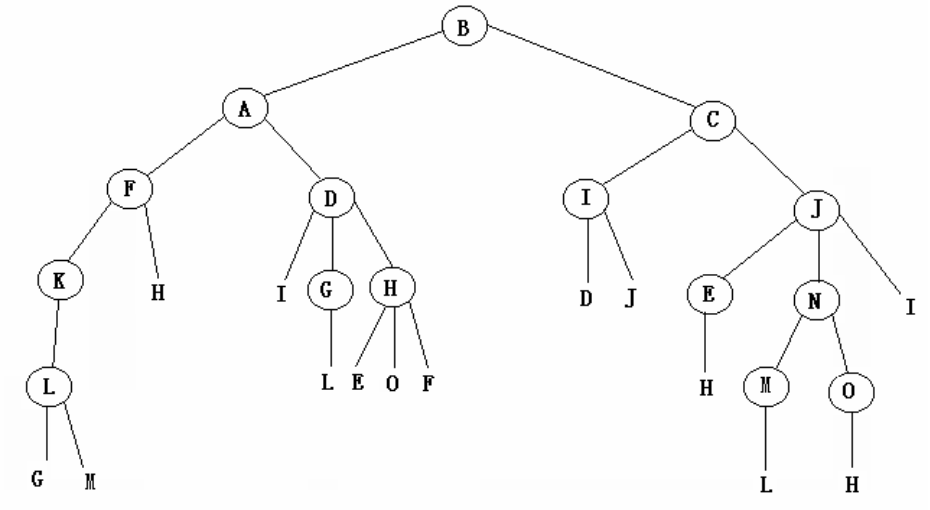


图 5-16 反向通路转发算法产生的树

（b）使用沉落树算法从图5-15（b）可以看出，需要4个跳段，总共产生14个分组。

34．在图5-17示出的子网中，对于由成员A、B、C、D、E、F、I和K组成的一组路由器，计算路由器C的多投点分布树。

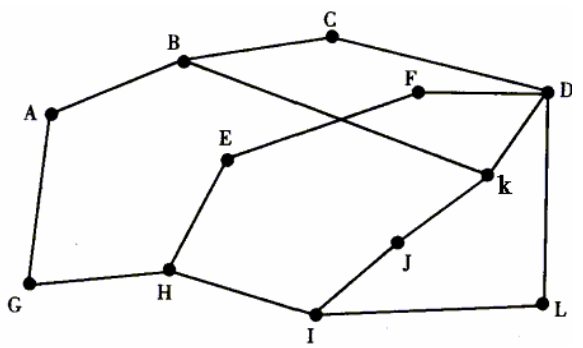


图 5-17　习题 34 插图

解答：有多个可能的分布树，图5-18列出的是其中的一个。

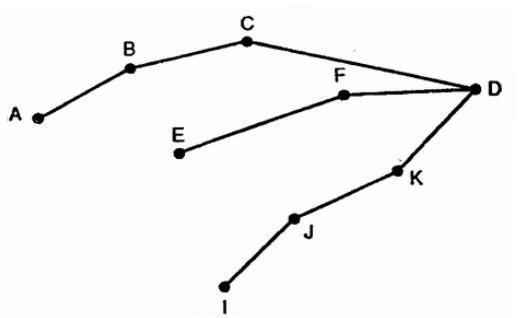


图 5-18　路由器 C 的多投点分布树

35．在内部使用虚电路的子网中，作为一种可能的拥挤控制机制，路由器可以抑制对收到的分组的应答，直到

（1）它知道它上次沿着该虚电路的发送被成功收到；
（2）它有一个空闲的缓冲区。

为简明起见，假定路由器使用停-等协议，并且每条虚电路为每个方向上的交通都配置一个专用的缓冲区。如果发送一个分组（可以是数据分组或确认分组）化T秒时间，并且在通路上有n个路由器，那么往目的地主机投递分组的速率是多少？假定传输差错极少发生，并且主机-路由器连接无限地快。

解答：对时间以T秒为单位分槽。在时槽1，源路由器发送第1个分组。在时槽2的开始，第2个路由器收到了分组，但还不能应答。在时槽3的开始，第3个路由器收到了分组，但也不能应答。这样，此后所有的路由器都不会应答。仅当目的地主机从目的地路由器取得分组时才会发送第1个应答。现在确认应答开始往回传播。在源路由器可以发送第2个分组之前，第1个分组需要两次穿行该子网，需要花费的时间等于2（n-1）T秒。所以，源路由器往目的地主机投递分组的速率是每2（n-1）T秒1个分组。显然，这种协议的效率是很低的。

36. 描述在警告位方法和RED（随机早期检测）方法之间的主要差别。

解答：在警告位方法中，通过在分组的头部设置一个特别的位传达警告信息。当分组到达目的地时，传输实体把该位拷贝到往回发给源的下一个应答分组中。然后源减少进入网络的交通量。只要路由器处于警告状态，它就继续把警告位置1，源就继续收到警告位置1的应答分组，并继续降低其发送速率。由于沿途的每个路由器都设置警告位，只有当没有路由器处于拥塞状态时，源才会再增加发送速率。

在随机早期检测方法中，在所有的缓冲区空间被用尽之前就开始丢弃分组。在像是TCP这样的运输协议中，对丢失分组的响应是让源减慢速度。这些协议通常是为有线网络设计的，有线网络非常可靠，分组丢失主要是由缓冲区溢出而不是由传输错误引起。RED正是利用这一事实来减少拥塞。其主要思想是在严重的拥塞发生之前能够有时间采取避免措施。为了确定什么时候开始丢弃分组，路由器维持一个队列长度平均运行值。当在某条线路上平均队列长度超过一个门槛值时，就认为该线路是拥塞的，并开始采取行动。怎样把拥塞状态通知给源呢？一种方法是给它发送一个拥塞分组。这种方法的问题是在已经拥塞的网络上加入更多的交通量。另一种不同的策略是仅仅丢弃选择的分组，不对它进行报告。源最终会注意到没有收到应答，从而采取行动，减慢发送速率，而不是重传。应该指出，在无线网络中，大多数分组丢失都不是由拥塞和丢弃分组产生，而是由空中链路上的噪音产生的，因此本方法不能使用。

综上所述，在两种方法之间的主要差别是：

（1）警告位方法通过把一个位置1，明确地给源发送一个拥塞通告，而RED方法通过简单地丢弃分组隐含地向源通告拥塞状态。

（2）警告位方法在没有剩余缓冲区空间时才会丢弃分组，而RED方法在缓冲区用完之前就丢弃分组。

37．一个数据报子网允许路由器在需要的时候丢弃分组。一个路由器丢弃一个分组的概率是p。现在考虑这样一种情况，一个源主机连接到源路由器，后者又连接到目的地路由器，然后再连接到目的地主机。如果任一路由器丢弃一个分组，源主机最终会发生超时事件，并重发分组。如果主机-路由器和路由器-路由器线路都算作跳段，并且不考虑除路由器以外其它丢弃分组的可能性，那么试问：

（a）每次发送一个分组行走的平均跳段数是多少？

（b）一个分组平均做多少次发送？

（c）每个接收到的分组平均走了多少个跳段？

解答：由源主机发送的每个分组可能行走1个跳段、2个跳段或3个跳段。走1个跳段的概率是p，走2个跳段的概率是p（1-p），走3个跳段的概率是（1-p）^{2}，那么，一个分组平均通路长度的期望值是这3个概率的加权和，即等于L=1×p+2p（1-p）+3（1-p）^{2}=p^2-3p+3。

即每次发送一个分组行走的平均跳段数是p^2-3p+3。注意，当p=0时，平均长度是3，当p=1时，平均长度是1。当0<p<1时，可能需要多次发送。

一次发送成功（走完整个通路）的概率等于（1-p）^{2}，令α=（1-p）^{2}，两次发射成功的概率等于（1-α）α，三次发射成功的概率等于（1-α）^{2}α，…。因此，一个分组平均发送次数就等于

T=α+2α（1-α）+3α（1-α）^{2}+…

=[α/（1-α）][（1-α）+2（1-α）^{2}+3（1-α）^{3}+…]

因为

$$\sum_{k=1}^{\infty} kq^k = \frac{q}{(1-q)^2}$$

所以

$$T=\frac{\alpha}{1-\alpha}\cdot\frac{1-\alpha}{[1-(1-\alpha)]^2}=\frac{1}{\alpha}=\frac{1}{(1-p)^2}$$

即一个分组平均做1/（1-p）^{2}次发送。

最后，每个接收到的分组行走的平均跳段数等于H=L×T=（p^2-3p+3）/（1-p）^{2}。

38．在一个特别的系统中使用了字节计数类的漏桶算法。其规则是在每一个滴答时间上可以发送1个1024字节的分组，两个512字节的分组等等。试给出该系统一个严重的限制。

解答：不可以发送任何大于1024字节的分组。

39．原始漏桶算法很简单。漏桶由一个有限队列构成。当分组到达时，如果队列未满，将其加到队尾；否则丢弃它。每个时钟节拍发送一个分组（除非队列为空）。请说明漏桶算法为什么每个滴答时间允许一个分组进入网络，而不考虑分组的大小。

解答：通常计算机能够以很高的速率产生数据，网络也可以用同样的速率运行。然而，

路由器却只能在短时间内以同样高的速率处理数据。对于排在队列中的一个分组，不管它有多大，路由器必须做大约相同份量的工作。显然，处理10个100字节长的分组所做的工作要比处理1个1000字节长的分组所做的工作多得多。

40．在令牌漏桶算法中，漏桶可以保留令牌。由一个时钟每隔△T秒生成一个令牌，每传送一个分组，就必须得到和消耗一个令牌。例如对于一个保留着3个令牌的桶，如果有5个分组等着传送，那么5个分组中的3个可以被立即传送出去，但其余2个必须等待新令牌的生成。现在有一个ATM网络使用令牌漏桶方案管制交通。每5微秒钟放入漏桶一个新的令牌。试问最大的可持续的净数据速率（即不包括头位）是多少？

解答：每5微妙产生1个令牌，1秒=10^6微妙，1秒钟可以发送2×10^5个信元。每个信元含有48个数据字节，即8×48=384个比特。$384\times2\times10^5=76.8\times10^6$bps

所以，最大的可持续的净数据速率为76.8Mbps。

41．在一个6Mbps网络上的一台计算机受到令牌漏桶的交通管制。假定令牌填入速率为1Mbps，开始时漏桶装填的容量是8M位。那么，计算机可以用完全速率6Mbps发送多长时间？

解答：本题乍看起来，似乎以6Mbps速率发送用4/3秒时间可以取完桶内8M位的数据，使漏桶变空。然而，这样回答是错误的，因为在这期间，已有更多的令牌到达。正确的答案应该使用公式S=C /（M-P），这里的S表示以秒计量的突发时间长度，M表示以每秒字节计量的最大输出速率，C表示以字节计的桶的容量，P表示以每秒字节计量的令牌到达速率。用$C=8\times10^6\div8=10^6$，$M=6\times10^6\div8$　$P=1\times10^6\div8$ 代入公式得到

$$S=\frac{10^6}{6\times10^6\div8-1\times10^6\div8}=1.6\text{（秒）}$$

因此，计算机可以用完全速率6Mbps发送1.6秒的时间。

42．下面列出的是一种流描述（flow specification）的4个输入特征：

- 最大分组尺寸（字节）
- 令牌桶速率（字节/秒）
- 令牌桶大小
- 最大传输速率（字节/秒）

现在假定最大分组尺寸是1000字节，令牌桶速率是10M字节/秒，令牌桶大小是1M字节，最大传输速率是50M字节/秒，问以最大速率突发传送可维持多长时间？

解答：令最大突发时间长度为Δt秒。在极端情况下，漏桶在突发期间的开始是充满的（1M字节），在突发期间另有10Δt M字节进入桶内。在传输突发期间的输出包含50Δt M字节。由等式1+10Δt=50Δt，得到Δt=1/40秒，即25毫秒。因此，以最大速率突发传送可维持25毫秒的时间。

43．一个设备从它所连接的以太网接收帧，它取出每个帧内的分组，为分组加上成帧信息，并通过一条租用电话线（对外部世界的唯一连接）把帧发送到另一端同样的设备。在另一端，该设备解开帧，并把分组插入到令牌环帧，再在令牌环局域网上把帧发送到一个当地主机。你把这种设备叫什么名字？

解答：因为不涉及路由选择（仅有一条电话线），所以该设备是半桥。

44．在串接的虚电路互连网络中也需要分割吗？还是仅仅在数据报系统中需要分割（fragmentation）处理？

解答：在这两种情况下都需要分割功能。即使在一个串接的虚电路网络中，沿通路的某些网络可能接受1024字节分组，而另一些网络可能仅接受48字节分组，分割功能仍然是需要的。

45．通过一个串接的虚电路子网的隧道是直接的，在一端的多协议路由器只需建立一条虚电路到达另一端的多协议路由器，并通过该虚电路传送分组。隧道也可以用于数据报子网吗？如果可以，如何使用？

解答：可以。只需把分组封装在属于所通过的子网的数据报的载荷段中发送即可。

46．图5-19示出了在ATM网络中建立虚电路和释放虚电路的过程。我们可以把网络和主机之间的交互使用四类原语进行分类，这四类原语是：请求、指示、响应和证实。试把图中的SETUP和CONNECT报文划分进这些类别。

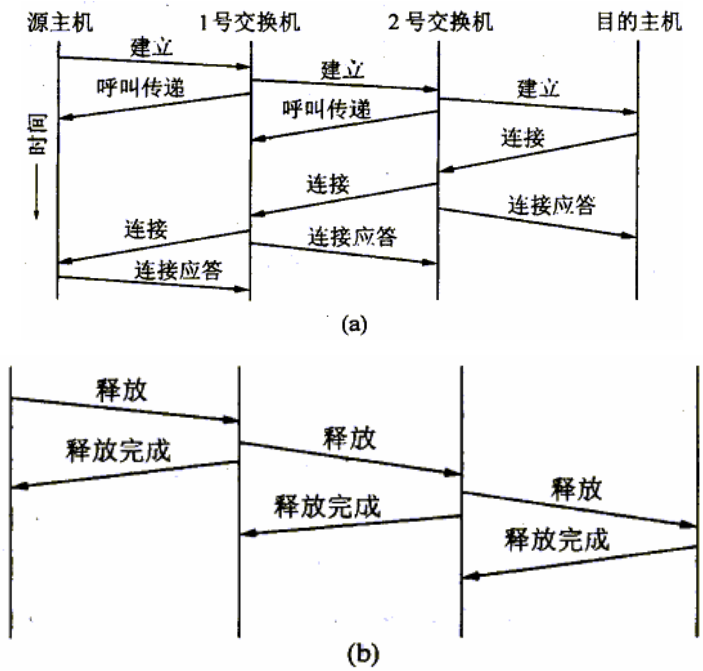


图 5-19　ATM 网络中的连接建立和连接释放

解答：SETUP（建立）报文当被源发送时是一个请求，但当它到达目的地时则是一个

指示。CONNECT（连接）当被目的地发送时是一个响应，但当它被源收到时则是一个证实。

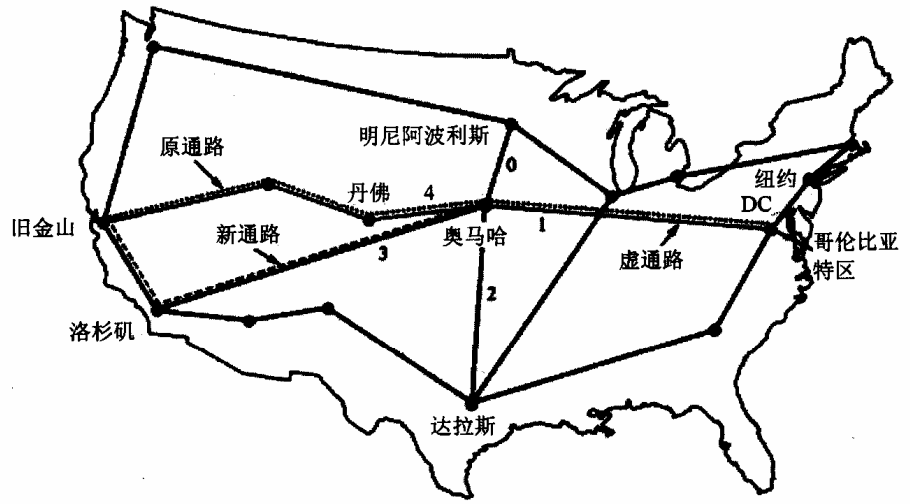
47．在一个ATM网络中建立一条新的虚电路。在源和目的地主机之间有3个ATM交换机。为了建立这个虚电路将要发送多少个报文（包括确认报文）？

解答：让SETUP报文到达目的地需要4个跳段，除了最后1个跳段外，每个跳段都被确认，这样共有7个报文。类似地，CONNECT报文也经历4个跳段，并且有4个确认，共有8个报文。因此，全部加在一起，总共需要发送15个报文。

48．在一条ISDN B信道上以传真的方式传送一幅8×10英寸图象要花多少时间？假设传真机把每英寸数字化为300个象素，每个象素用4比特表示。当前的传真机在普通电话线上比这要快，你认为我们是怎样做到的？

解答：这幅图象有8×10=80平方英寸，总共有（8×300）×（10×300）=7200，000个象素。每个象素用4比特表示，总的数据量为4×7200000=28.8 M比特，即28800k比特。在ISDN B信道上以64kbps速率发送，所需花的时间是28800÷64=450秒。当前的FAX机器每个象素仅使用1比特，节省了一个因子4，但当前的FAX调制解调器运行速率是14.4kbps，不是64kbps，因此发送一个整页仍需450秒。它们看起来比较快的原因是因为大多数页的百分之九十五是空白，而所使用的行程编码把这些空白全部删除了。

49．图5-20示出了通过奥马哈（Omaha）市的ATM交换机的一些路由。建立该表所用的逻辑是简单的：总是把尚未使用的最低VPI分配给一条新的连接。如果在纽约（NY）和丹佛（Denver）两个节点之间请求一条新的虚电路，该虚电路将会被分配给哪一个VPI？



源	入口栈	入口 VPI	目的地	出口栈	出口 VPI	通路
纽约	1	1	旧金山	4	1	新
纽约	1	2	丹佛	4	2	新
洛杉矶	3	1	明尼阿波利斯	0	1	新
哥伦比亚特区	1	3	洛杉矶	3	2	新
纽约	1	1	旧金山	4	1	旧
旧金山	4	3	哥伦比亚特区	1	4	新
哥伦比亚特区	1	5	旧金山	4	4	新
纽约	1	2	丹佛	4	2	旧
旧金山	4	5	明尼阿波利斯	0	2	新
纽约	1	1	旧金山	4	1	旧

图 5-20 通过奥马哈（Omaha）市的 ATM 交换机的一些路由

解答：那个通路已经存在，并且具有VPI 2。从NY到Denver的一条新的虚电路将使用该通路，并被分配VPI 2（当然了，应该使用不同的VCI）。

50．在图5-21中，如果一个信元提前到达，下一个信元仍然预期在t1+2T到达。假定采用不同的规则，即下一个信元改成预期在t2+T到达，并且发送方最大限度地。那么，可以取得的最大峰值信元速率是多少？假定T=10微妙，L=2微妙，请分别给出原来的和新的峰值信元速率。

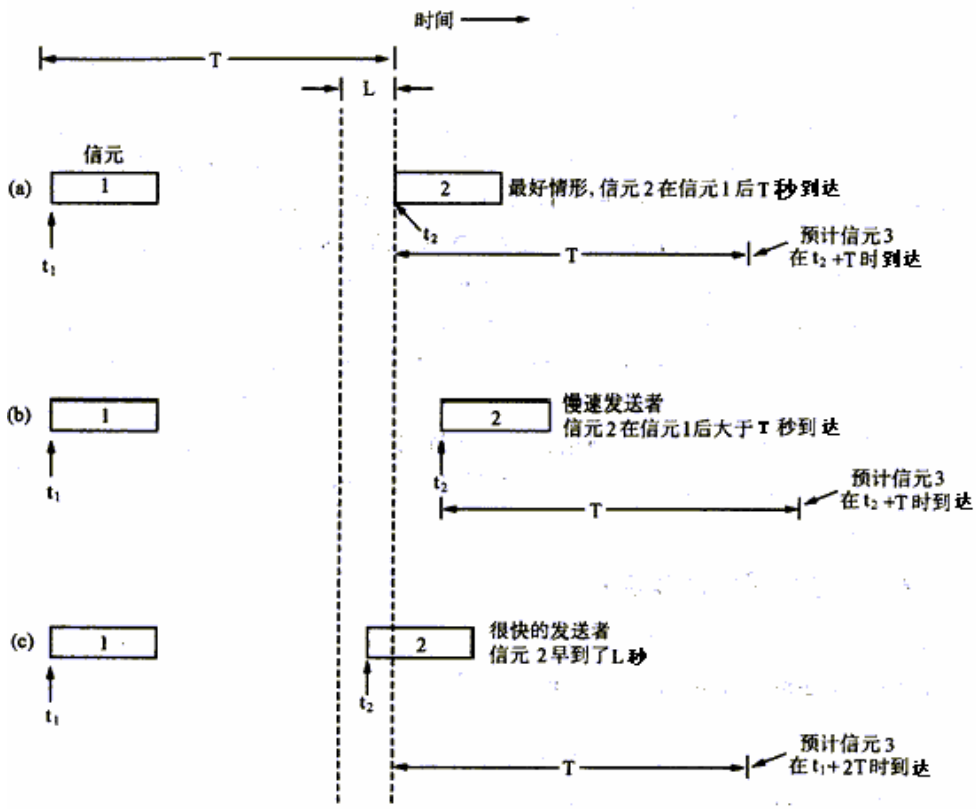


图 5-21　通用信元速率算法

解答：在效果上，现在的到达时间间隔是T-L，因此，峰值速率由1/T增加到1/（T-L）。对于T=10微妙，L=2微妙，峰值速率将以每秒10^5个信元增加到每秒125000个信元。

51．一条155.52Mbps ATM ABR连接的PCR值是200000，L值是25微妙。试问该连接的最大突发长度是多少个信元？

解答：这里需要使用通用信元速率算法（GCRA：Generic Cell Rate Algorithm）.GCRA通常有两个参数，即T和L。T就是PCR（信元发送的最大速率）的倒数，L就是CDVT（可接受的最大信元抖动，即可容忍的信元延迟的最大变化）。假定每个遵守交通协定的信元的到达都要往漏桶中加入T个单位的水。漏桶以每秒1个单位的速率漏水，那么水漏光需T秒时间。在连续突发N个信元期间，加到漏桶的水的总量是NT，因为每个信元都加入T个单位。我们把信元发送时间计作δ，并且让δ≤T。在突发N个信元期间，漏掉的水的数量等于（N-1）δ，因为在第1个信元被完全发送出去之前，泄露不会开始。

在最大的连续突发期间，桶中水的净增量为NT-（N-1）δ。漏桶容量是T+L。令

NT-(N-1)δ=T+L

得到

$$N=1+\frac{L}{T-\delta}$$

现在，T=1/PCR=10^6 ÷200000=5微妙，L=25微妙

信元发送时间为：δ=53×8 ÷155.52≈2.73微妙，代入上列公式后，得到连续发送的信元数

N=12.01，约为12。

因此，该连接的最大突发长度是12个信元。

52．试举出在ISDN网中NT12（相对于NT1和NT2）的一个优点和一个缺点。

解答：在ISDN的拓扑结构中，NT1设备包括跟在用户建筑物内ISDN物理的和电气的端接相关的功能。NT1可以由ISDN提供者控制，形成到达网络的一个边界。这个边界把用户跟订户回路的传输技术隔离开来，并为附接用户设备提供物理连接器接口。此外，NT1执行诸如回路测试和性能监视等线路维护功能。NT1支持多个通道（例如2B+D）；在物理层，使用同步时分复用技术，把这些通道的位流复用在一起。NT1接口可以通过多投点配置支持多个设备，例如一个住户接口可能包括一部电话、一台个人计算机和一个报警系统，所有这些设备都通过一条多投点线路附接到单个NT1接口。

NT2是一个智能设备，能够执行交换和集中功能；它可以包括OSI模型直至第3层的功能。NT2的例子包括数字PBX，终端控制器和局域网。

NT1和NT2设备可以被结合成单个设备，称作NT12。该设备处理物理层、数据链路层和网络层功能。

NT12的优点是比较便宜，但是如果线路技术改变了，整个的设备必须更换。

53．在图5-22中，我们看到在通过榕树交换机的信元之间有冲突，冲突出现在第1级和第2级。在第3级也可能发生冲突吗？如果可能，在什么条件下发生？

解答：为了能够解答本题，首先要熟悉榕树交换机的工作机制。榕树交换机的取名源自它与榕树根的相似性。在所有的榕树交换机中，每条输入线路到每条输出线路间仅有一条路径。路由选择是通过为每个信元寻找输出线路来完成的（基于虚电路信息和表）。以图5-23示出的8×8的3级榕树交换机为例，3比特的二进制数被放在每个信元的开头，它将被用于在交换机内部寻找路由。这3个比特对应一个输出线路号。当一个信元到达一个交换单元时，该单元检查输出线路号的一位，并基于该信息将该信元传送到端口0（上面的端口）或端口1（下面的端口）。如果发生冲突，那么一个信元被发送，而另一个被抛弃。

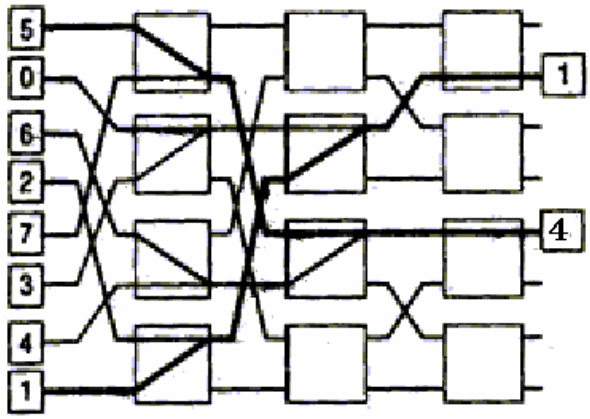


图 5-22　在一个榕树交换机中的单元碰撞

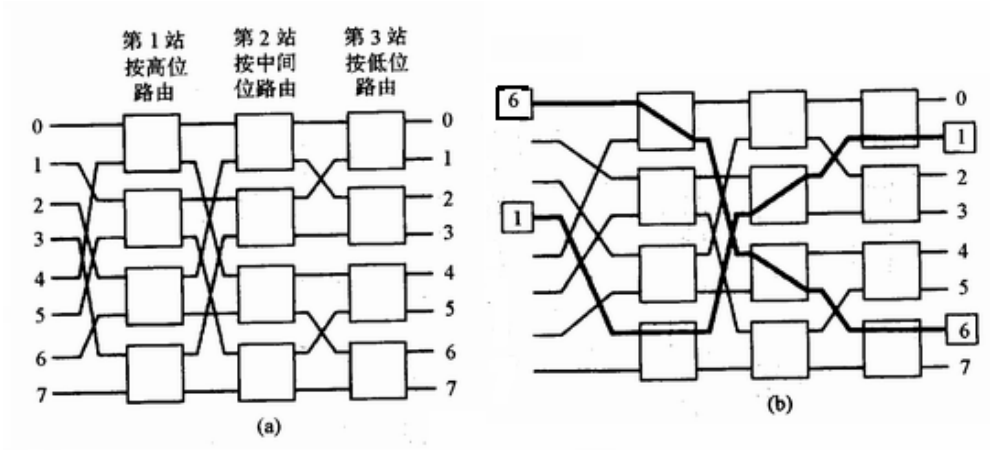


图 5-23　（a）具有 8 个输入线路和 8 个输出线路的榕树交换机

（b）两个信元通过榕树交换机的路由

榕树交换机自左向右分析输出线路号，第1级检查最左面的位（高位），第2级检查中间位，第3级检查最右边的位（低位）。在图5-23（b）中，我们看到有两个信元：在输入线路0上有一个信元前往输出线路6；在输入线路3上有一个信元前往输出线路1。对于第一个信元，二进制输出地址是110，因此它分别使用下、下和上端口通过三级。类似地，标为二进制001的另一个信元分别使用上、上和下端口通过三级。

当2个输入信元想在同一时间通过同一交换机单元的同一端口时会发生冲突。图5-22示出了一系列这样的冲突。在第1级，冲突涉及前往下列输出线路对的信元：（5，7），（0，3），（6，4）和（2，1）。假定这些冲突是以偏向于5、0、4和1来解决的。在第2级，我们会看到（0，1）冲突和（5，4）冲突。这里我们让1和4得胜，则它们将被送到正确的输出线路。

在第3级发生冲突也是可能的，但仅当两个信元都前往同一输出线路时才会发生。如果它们前往不同的输出线路时，不可能有冲突发生。

54. 在这个问题中，你需要为一些信元选择路由，一步一步地通过一个白切尔-榕树ATM交换机。有4个信元在输入线路0至3上，分别前往3、5、2和1。对于6级白切尔交换机的每一级和4级榕树交换机中的每一级（包括输入和输出），以8元组的形式列出有哪些信元在那里（在线路0上的信元，在线路1上的信元，…，等等）。没有信元的线路用-表示。

解答：在白切尔-榕树交换机背后的思想是在榕树交换机前面放置一个交换机，让它把信元排列成榕树交换机可以不丢弃信元的配置。例如，在图5-24中，如果输入信元按照目的地顺序排列出现在输入线0、1、2、3、4、5、6、7上，这样榕树交换机就不会丢弃信元。

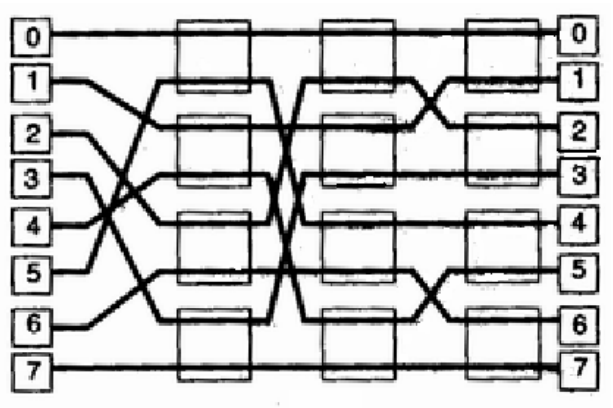


图 5-24　通过榕树交换机的无冲突路由

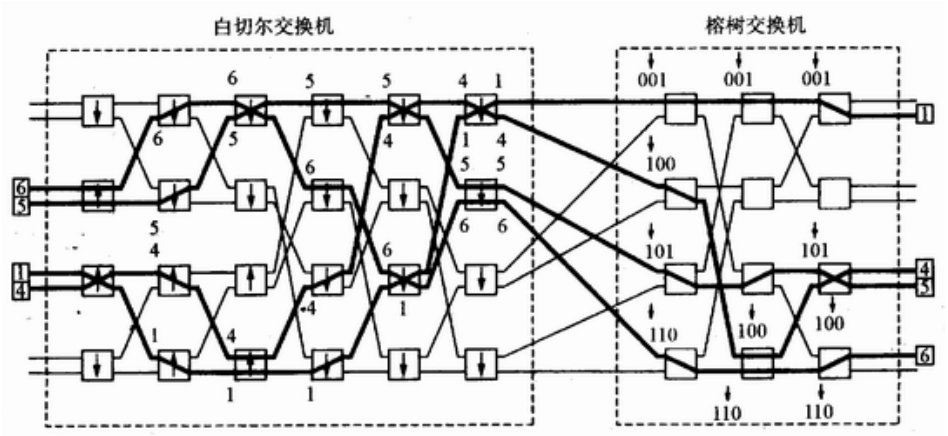


图 5-25　使用白切尔-榕树交换机有 4 个信元的示例

为了排序输入的信元，我们可以使用白切尔交换机。与榕树交换机一样，它也是同步的，并且使用离散的周期。白切尔交换机由2×2的交换单元构成，但是其工作方式和榕树交换机不一样。当交换机单元收到两个信元时，它比较它们的输出地址的大小（不是仅比较比特），并且将地址大的一个输出到箭头所指的端口，地址小的一个输出到另一个端口。如果仅收到一个信元，它会走向与箭头所指方向相反的端口。

如图5-25所示，作为例子，信元出现在输入线路2、3、4和5上，其输出线路分别为6、5、1和4。粗线示出了到输出端的所有路径。在白切尔交换机的末端4个信元都在顶端排好

了序，然后它们通过一个混合网络，并且进入榕树交换机，后者无冲突地处理它们。

本习题中的初始状态是（3 5 2 1 - - - -）。通过白切尔网络的6级分别出现下列8元组：

（3，2，5，1，-，-，-，-）
（2，1，3，5，-，-，-，-）
（1，-，2，-，3，-，5，-）
（1，3，-，-，2，5，-，-）
（1，2，3，5，-，-，-，-）
（1，2，3，5，-，-，-，-）

因此，信元被正确地排序，并被放置到顶部。

对应于榕树交换机的4级，信元8元组分别为：

（1，-，2，-，3，-，5，-）
（1，3，2，-，-，-，-，5）
（1，-，3，2，-，5，-，-）
（-，1，2，3，-，5，-，-）

显然，这是正确的交换结果。

55．重复上一问题，但输入为（7，-，6，-，5，-，4，-）。

解答：参照图5-26，对应于白切尔交换机的6级的八元组是：

（7，-，-，6，-，4，5，-）
（7，6，-，-，-，-，4，5）
（6，-，7，-，-，5，-，4）
（6，5，-，-，7，4，-，-）
（5，4，6，7，-，-，-，-）
（4，5，6，7，-，-，-，-）

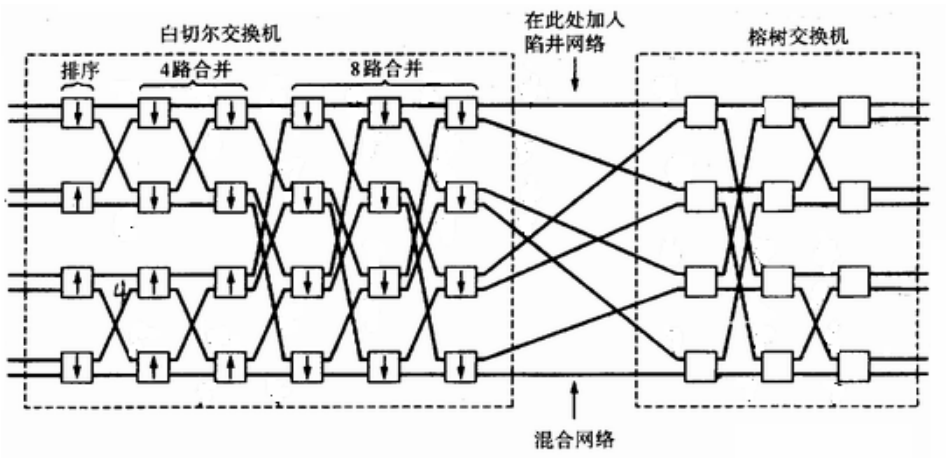


图 5-26　白切尔-榕树交换机的交换结构

对应于榕树交换机的4级（包括输入和输出）的八元组是：

（4，-，5，-，6，-，7，-）
（-，-，-，-，4，6，5，7）
（-，-，-，-，4，5，6，7）
（-，-，-，-，4，5，6，7）

这也是所预期的结果。

56．一个ATM交换机有1024条输入线路和1024条输出线路。线路按照SONET的622Mbps速率运行，这样用户速率大约为594Mbps，则交换机总的带宽应该有多少？它每秒至少可以处理多少个信元？

解答：OC-1速率51.84Mbps中除去段开销、线路开销和通路开销。用户数据传输速率为49.536Mbps。

SONET的622Mbps对应于OC-12，因此相应的用户数据传输速率为

49.536×12=594.432≈594Mbps。

594×1024=608256Mbps，约为608Gbps

608÷8÷53≈1.43

所以，交换机的总带宽为608Gbps，它每秒至少可以处理1.43千兆个信元。

57. 试举出帧中继相对于租用电话线路的一个优点和一个缺点。

解答：帧中继的一个缺点是用户不能够在全天所有的时间内以全速发送数据。它的一个优点是比较便宜。仅当你需要用它的时候，它才像是在起一条租用线路的作用。

58. 某网有50个IMP（接口信息处理机）节点，延时用8位二进制数来记录交换的延迟时间，每秒交换4次，问分布式路由算法对每条（全双工）线路耗费多大带宽？

解答：路由表的长度等于8×50=400比特。该表每秒钟在每条线路上发送4次，因此，400×4=1600bps，即在每条线路的每个方向上消耗的带宽都是1600bps。

59. 在一个路由器中的CPU每秒可以处理200万个分组。提供给它的负载是每秒150万个分组。如果从源到目的地的路径包含10个路由器，那么由CPU排队和服务共花了多少时间？

解答：乍看起来，如果路由器处理1个分组花1微秒的时间，那么它每秒钟就可以处理100万个分组。但实际上往往并非如此，因为由于负载的统计式波动总会有空闲周期。如果CPU需要在每一周期内完成一项工作，那么由于偶然的空闲错过了几个周期，就会产生积累工作总是没有机会去做。

即时对于略低于理论容量的负载，队列中也可能有积累，也会产生延迟。考虑这样一种情况，分组以每秒λ个的平均到达速率随机地到达。每个分组所需要的CPU时间也是随机的，假定平均处理量是每秒λ个分组。在这样的假定条件下，到达分布和服务分布都是Poisson分布。使用队列理论可以证明，一个分组所经历的平均延迟时间是

$T=(1/\mu)\times 1/(1-\lambda/\mu)=1/\mu\times 1/(1-\rho)$，

在这里，$\rho=\lambda/\mu$是CPU的利用率。第1个因子是在无竞争的条件下1个分组的平均服务时间。第2个因子是由于跟其它流的竞争引起的变慢程度。例如，如果λ=950，000分组/秒，μ=1 000 000分组/秒，那么，ρ=0.95，每个分组所经历的平均延迟将增加到20倍，在前面举的例子中，就由1微秒增至20微秒。这个延迟时间既考虑了队列时间，也考虑了服务时间。显然，当负载非常低（$\lambda/\mu\approx 0$）时，T值接近于$1/\mu$。

在本题中，$\mu=2\times 10^6$分组/秒，因此$\rho=\lambda/\mu$=0.75，$1/(1-\rho)$=4，这样根据排队理论，每个分组经历的延迟是空闲系统的4倍。

$1/\mu=1/(2\times 10^6)=0.5$微妙，　0.5×4=2微秒

沿着通路有10个路由器，排队加服务的时间是20微秒。

第 6 章　IP 网络

本章学习重点

- IP地址
- 地址映射
- IP分组
- IP路由选择
- 互连网控制报文协议
- 可变长子网掩码
- 无类别域间路由选择
- 移动IP
- IPv6
- 组播
- 集成服务和差分服务
- 多协议标记交换

6.1　基本知识点

互联网协议（IP）使得通过众多的基于不同技术的异种网络的通信成为可能。连接到Internet的任何主机可以跟也连接到Internet的任何其它主机通信。因此，Internet提供了普遍存在的连接性以及由于大量采用所产生的规模经济。

IP协议涉及建成互连网所需的通信协议软件，正是这些软件把基础物理传输机制隐藏起来，进行统一的合作网络的互连，支持一种通用的通信服务。在每一个网络内部，计算机使用基础的依赖于技术的通信设施。我们在依赖于技术的通信机制和应用程序之间插入的网际互连软件隐藏低层的细节，使得集成网络看起来象是单个大的网络。这样一种互连方案就称为网际互连，所形成的网络称为inernet（互连网）。

我们希望能够通过中间网络发送数据，即使这些中间网络与源发主机和目的地计算机没有直接的连接。为了建立一个有生命力的互连网，我们需要某些计算机能自动把报文以分组形式从一个网络转发到另一个网络。互连两个网络并且将报文分组从一个网络传递到另一个网络的计算机叫做网关或路由器。

IP最基本的服务是提供一个非可靠的尽最大努力去完成好任务的、无连接的分组投递系统。说它非可靠，是因为所要求的投递不能保证成功，分组可能丢失，投递无序或重复投递，而IP并不检测这些情况，发生这些情况也不通知发送者或接收者。说它无连接，是

因为每一个分组的外理都独立于其它分组，一串分组从一个机器发出，可以经由不同的路经到达另一机器，也可能部分分组丢失了，而其余的仍被投递。说这种服务是尽最大努力做好的，因为IP尽最大努力去投递分组，并不轻易地抛弃分组，仅当资源用尽或下面的物理网失效时才会发生不可靠的现象。

IP协议定义数据传送的基本单元——IP分组及其确切的数据格式。IP协议也包括一套规则，指明分组如何处理，错误怎样控制。特别是，IP协议还包含非可靠投递的思想，以及与此关联的分组路由选择的思想。

6.1.1 IP地址

internet协议地址（简称IP地址）对网上的某个节点来说是一个逻辑地址。它独立于任何特定的网络硬件和网络配置，不管物理网络的类型如何，它都有相同的格式。IP地址是一个4字节的数字，实际上由两部分合成，第一部分是IP网络号，第二部分是主机号。这种4字节的IP地址通常以小圆点分隔，其中每个字节都用十进制数字表示，如130.130.71.1，其网络号是130.130，主机号是71.1。在某些场合，IP地址也以十六进制数字表示，如0×82.0×82.0×47.0×01。

IP地址可分成五类，即A类、B类、C类、D类和E类。用二进制代码表示，A类地址的最高位等于0,B类地址的最高两位等于10，C类地址的最高三位等于110，D类地址的最高四位等于1110，E类地址的最高五位等于11110，由于D类地址仅用于主机组的特殊定义，E类地址作为保留未来使用的地址，故具体网络只能分配A类、B类、C类地址中的一种。

因为IP地址既对一个网络编码，也对那个网络上的一台主机编码，所以，它们不是确定单个主机，而是确定对一个网络的一条连接。

使用IP地址的单位可以把它们的网络划分成几个部分，每个部分称为一个子网。每个子网对应于一个下属部门或一个地理范围（比如一座或几座办公楼），或者对应一种物理通信介质（比如以太网，点到点连接线路或X.25网）。它们通过网关互连或进行必要的协议转换。

首先，要确定每个子网最多可包含多少台主机，因为这将影响32位IP地址中子网号和主机号的分配。比如，B类地址用开头2字节表示网络号，剩下2个字节是本地地址。如果拥有该IP网的单位的计算机数目不超过57316（=14×4094）台，它就可以用主机号的开头4位做子网号。这种划分（即用主机号部分的开头4位做子网号）允许该单位有14个子网，每个子网最多可以挂4094台主机，再如，拥有B类IP地址的单位在下属部门较多，每个部门配备的计算机数量较少的情况下，也可以用主机号的开头一个字节做子网号，从而允许该单位有254个子网，每个子网最多可以挂254台主机。

当一个IP分组从一台主机送往另一台主机时，它的源和目标地址被一个称做掩码的数码屏蔽。子网掩码的主机号部分是0，网络号部分的二进制表示码是全1，子网号部分的二进制表示码也是全1。

6.1.2　地址映射

地址解析协议（ARP）用来将IP地址翻译成物理网络地址。考虑两台计算机A和B共享一个物理网络的情况。每台计算机分别有一个IP地址IA和IB，同时有一个物理地址PA和PB。设计IP地址的目的是隐蔽低层的物理网络，允许高层程序只用IP地址工作。但是不管使用什么样的硬件网络技术，最终通信总是由物理网络实现的。IP模块建立了IP分组，并且准备送给以太网驱动程序之前，必须确定目的地主机的以太网地址。

TCP/IP协议设计人员采用一种创造性的方法，解决了诸如以太网这样具有广播能力物理网络的地址转换问题。为避免依赖一个映射表，他们选择一种低层协议，动态地映射地址，这就是所谓的地址解析协议（ARP）。从IP地址到物理地址的变换是通过查表实现的，ARP表放在内存储器中，其中的登录项是在第一次需要使用而进行查询时通过ARP协议自动填写的。

如果IP模块在ARP表中找不到某一目标IP地址的登录项，它就使用广播以太网地址发一个ARP请求分组给网上每一台计算机。这些计算机的以太网接口收到这个广播以太网帧后，以太网驱动程序检查帧的类型段（值0806表明是一个ARP分组），将相应的ARP分组送给ARP模块。这个ARP请求分组说：“如果你的IP地址跟这个目标IP地址相同，请告诉我你的以太网地址”。

收到广播的每个ARP模块检查请求分组中的目标IP地址，当该地址和自己的IP地址相同时，就直接发一个响应分组给源以太网地址。ARP响应分组说：“是的，那个目标地址是我，让我来告诉你我的以太网地址”。

ARP又叫以太网ARP，原本就是为以太网制定的，但是在具有类似机制的其它网络上同样可以运用。

6.1.3　IP分组

互连网协议（IP）的目的是提供必要的功能，使一个个IP分组从源发主机通过网络互连系统传递到目的地主机。IP分组也称IP数据报，它是以无连接方式通过网络传输的。无连接的意思就是指在数据传输之前源节点与目标节点并不建立连接。

在IP分组的传递过程中，不管行走多长的距离，或跨越多少个物理网络，IP模块的寻址机制和路由选择功能都能保证将数据送到正确的目的地。所经过的各个物理网络可能采用不同的链路协议和帧格式，但是，无论是在源发主机和目的地主机中，还是在路过的每个路由器中，网络层都使用始终如一的协议（IP协议）和不变的分组格式（IP分组）。

在一个物理网络上传送的单元是帧，帧包含头和数据，头给出了源和目标地址类的信息。而internet称基本传送单元为IP分组。类似典型的物理网络帧，IP分组也分头和数据区，分组的头包含源和目的地地址。当然，不同点在于IP分组包含的是IP地址。

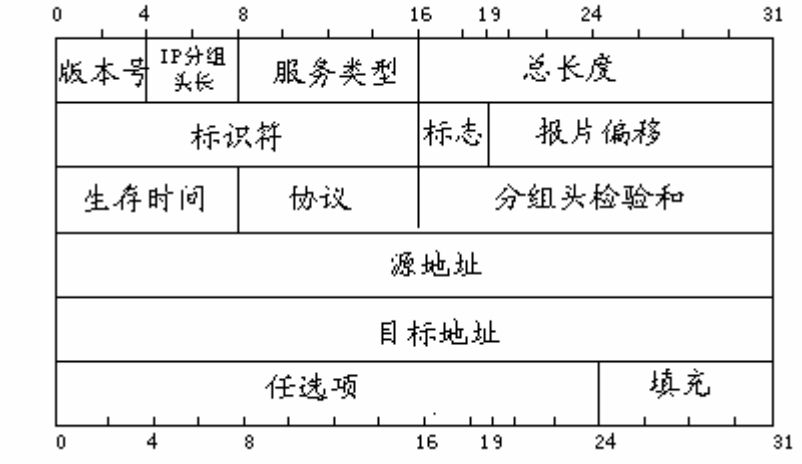


图 6-1　IP 分组头

如图6-1所示，IP分组头的长度为4个字节（32位）的整数倍。从任选项往后是可变长部分，这一部分也可以没有。以下列出的是分组头中的各个段的含义。

4位的版本号 段表示协议支持的IP版本号。

4位的互连网分组头长 表示IP分组头的长度，以32个二进制位（4个字节）为单位，取值的范围是5-15（缺值是5）。由于IP分组头的长度是可变的，故这个段是必不可少的。

8位的服务类型段说明分组所希望得到的服务质量。它允许主机指定在网络上传输分组的服务种类，也允许选择分组的优先级，以及希望得到的可靠性和资源消耗。该段的目的是请求网络提供所希望的服务。

16位的总长度段给出IP分组的总长度，单位是字节，包括分组头和数据的长度。数据段的长度可以从总长度减去分组头长度计算出来。由于总长度段有16位，所以最大IP分组允许有65535个字节。IP规范规定，所有主机和路由器至少能支持576字节的分组长度。如果IP分组在网络传送过程中被分成报片，那么分片后形成的IP分组中的 总长度段指的是单个报片的总长度，而不是原先IP分组的总长度。

16位的标识符段包含一个整数，唯一地标识IP分组。IP分组在传输时，其间可能会通过一些子网。这些子网允许的最大协议数据单元（PDU）长度可能小于该IP分组的长度。为了处理这种情况，IP为以数据报方式传送的IP分组提供了分片和重组的功能。这也正是IP模块的主要功能之一。当一个路由器分割一个IP分组时，要把IP分组头中的大多数段值拷贝到每个分组片中，标识符段必须拷贝。它的基本目的是使得目的地知道到达的哪些分组片属于哪个IP分组，源发方计算机必须为发送的每个IP分组分别产生一个唯一的标识符段值。为此，IP软件在计算机存储器保持一个全局计数器，每建立一个IP分组就加1，再把结果放到IP分组标识符段中。

3位的标志段含有控制标志。3位中的低序2位控制IP分组的分片，这2位分别称作不可分片位和还有分组片位；高序位没有被使用。当不可分片位置1时，规定不要将IP分组分片。仅当完整的IP分组才是有用的情况下，应用程序才可选择禁止分片。标志段的“还有分组片”位标明这个分组片包含的数据是取自原始IP分组中间，还是取自原始IP分组的最后。一旦

报宿收到一个分组片，如果它的“还有分组片”位置0，就知道这个报片中的数据取自原始分组的尾部。

13位的分组片偏移段标明当前分组片在初始IP分组中的位置。为了重组IP分组，报宿必须得到从偏移0开始，直到最高偏移值之间的所有分组片。这些分组片不需要按顺序到达，接收分组片的报宿与分割IP分组的路由器之间不进行通信，报宿也能重新组合IP分组。分组片偏移以64位（8个字节）为单位，取值范围0至8191，缺省值是0。

8位的生存时间段指定IP分组能在互连网中停留的最长时间，以秒为单位。当该值降为0时，IP分组就应被舍弃。该段的值在IP分组每通过一个路由器时都减去1。该段决定了源发IP分组在网上存活时间的最大值，它保证IP分组不会在一个互连网中无休止地往返传输。

8位的协议段表示哪一个高层协议将用于接收IP分组中的数据。高层协议的号码由TCP/IP中央权威管理机构予以分配。例如，该段值的十进制表示对应ICMP（互连网控制报文协议）是1，对应传输控制协议（TCP）是6，对应EGP（外部网关协议）是8，对应用户数据报协议（UDP）是17，对应ISO传输层协议第4类（ISO-TP4）是29。

16位的分组检验和段保证IP分组头值的完整性，当IP分组头通过路由器时，分组头发生变化（例如生存时间段值减1），检验和必须重新计算。检验和的计算十分简单。首先，在计算前将检验和段的所有16位均置成0，然后IP分组头从头开始每两个字节为一个单位相加，若相加的结果有进位，那么将和加1。如此反复，直到所有分组头的信息都相加完为止，将最后的值对1求补，即得出16位的检验和。

32位的源地址段包含发送IP分组的源主机的IP地址。32位的目标地址段包含IP分组的目的地主机的IP地址。

可变长的任选段提供了一种策略，允许今后的版本包含在当前设计的头中尚未出现的信息，也避免使用固定的保留长度，从而可以根据实际需要选用某些头部登录项。

填充段是为了使有任选项的IP分组满足4个字节长度的整数倍而设计的，通常用0填入填充段来满足这一要求。填充段的有无或所需要的长度取决于选择项的使用情况。

6.1.4　IP路由选择

一个TCP/IP网络是多个物理网络互连而成的，连接这些物理网络的路由器又常常称作网关。每个网关都有到两个或多个网络的直接连接。与网关不同，主机通常直接连到一个物理网上。为了区别连接网络的不同情况，我们把仅有一条线路直接连接到一个物理网络的节点称为端节点（end node），而将有两条以上的线路分别直接连接到多个物理网络的节点称为路由节点。

不管是端节点还是网关，它们都参与IP路由选择。当主机上的一个应用程序要进行通信时，TCP/IP协议产生一个或多个IP分组。我们将位于同一IP网上的两台计算机之间的通信称为直接路由通信，不位于同一IP网上的两台计算机之间的通信称为间接路由通信。

IP模块从高层接收数据，形成IP分组后，必须决定是直接还是间接发送该分组，并且选择一个低层网络接口，这些选择在访问路由表后作出。对于存在多个网关情况下的间接路由通信，主机还必须决定把IP分组送给本地网络上的哪个网关，因为没有一个网关能对所有目的地提供最好路径。当然，网关是要做路由选择决定的，这是它们的主要任务，这

也是它们同时被称为路由器的原因。

对于一个从底层接口收到的IP分组，IP模块必须决定是否将该分组传给上层模块；如果该分组需要转发给其它计算机，则与在本计算机建立的分组进行同样的发送处理。但是，对于从网上收到的IP分组，无论何时都不能沿原网络接口转发回去。

通常，Internet路由算法在每个机器上采用一张路由选择表，该表包含可能的目标信息。当一个IP分组到达一个网关时，IP软件就找到目标IP地址，抽出网络号，然后网关使用该网络标识决定路由。IP选择路由是基于目标网络号，而不是目标主机号。

在单个物理网络的两台机器之间，发送IP分组无需网关的转发功能，发送方将分组放在物理帧内直接传给目标机器。判断一目标地址是否在与本计算机直接连接的一个物理网络上的方法是，发送者抽出目标IP地址的网络部分，与自己IP地址的网络部分比较，如果相同，就直接投递。在本地网络划分子网的条件下，如果目标地址属于本地的另外一个子网，那么这里所说的IP地址的网络部分也包括子网号。

我们可以将IP路由选择算法归纳如下：

IP分组路由选择（IP分组，路由选择表）

从IP分组提取目标IP地址Id

计算目标网络的IP地址In

如果In与任何直接连接的网络地址一致，

则在那个网络上发送IP分组到目的地；

（包括将 Id转换成物理地址，封装IP分组和发送帧）

否则如果Id是主机特有的路由，则按表中指定的路由传送IP分组；

否则如果In 出现在路由选择表中，则按表中指定的路由传送IP分组；

否则如果指出了一条缺省路由，则选择将IP分组传送到缺省网关的路由；

否则宣布一个路由选择错误。

Internet是在广域网ARPANET的基础上发展起来。当Internet实验开始时，它以ARPANET作为其主干。所谓核心网关（core gateway）的思想就是将局部网络连接到ARPANET。对于路由选择来说，由单个管理当局控制的一组网络和网关称为自治系统，一个自治系统内的网关自由地选择它们自己的发现、传播、验证和检查路由一致性的机制。根据这一定义，核心网关也形成一个自治系统。

交换路由信息的两个网关如果属于两个不同的自治系统，那么就称它们是外部相邻；如果它们属于同一个自治系统，就称它们是内部相邻。外部网关用以通告可达性信息给其它自治系统的协议称为外部网关协议（exterior gateway protocol）或简称EGP。内部网关用以在一个自治系统内部交换网络可达性和路由选择信息的任何算法都称为内部网关协议（interior gateway protocol）或简称IGP。

BGP（边界网关协议）是一个广泛接受的EGP标准。许多路由器都使用BGP与由不同管理当局控制的采用不同设计或来自不同厂家的路由器互相通信。但一个自治系统内部的路由器之间的交互却没有统一的协议可用。之所以出现这种差异，一是在自治系统中所用的拓扑结构与所用技术的多样性，二是缺乏功能适宜、定义良好的早期标准。所以，只有非常少的协议得以流行，大部分自治系统使用这些少数协议中的一种在内部传播可达性信息。3种常用的内部网关协议分别称作路由选择信息协议（RIR:Routing Information

Protocol）、Hello和开放的SPF协议（OSPF：Open SPF Protocol）。

两个在自治系统间互相通信的BGP邻居必须在物理上属于一个网。在同一个自治系统内的BGP间的互相通信是为了保证它们对该自治系统有一致的了解，也是为了能够判定在那个自治系统内哪个BGP路由器将作为到达某个外部自治系统的连接点。BGP更新报文包括“网络号-自治系统路径”对信息。自治系统路径包括到达某个特别的网络须经过的自治系统序列，这些更新信息通过TCP传送出去，以保证其传输的可靠性。

RIP是广泛流传的IP路由选择算法实现之一，它是Berkeley UNIX发行软件中的一部分。RIP实现了距离向量算法，并使用跨度计量标准。一个跨度是直接连接的局域网，两个跨度是通过一个网关可达，3个跨度是通过两个网关可达。余此类推，但16个跨度被认为是最大极限，表示无穷距离，意即不可达。RIP运行于UDP之上，对于报文的目的地使用UDP周知口520号。实现RIP协议的路由器每隔30秒给它的邻居发送一个更新报文。为了应付诸如链路失效这样的拓扑变化，在最坏的情况下路由器期待在180秒内从它的邻居接收一个更新报文。如果路由器在限期内没有接收到邻居X的更新报文，它就假定到X的直接链路失效了，并把相应的最小代价设置成无穷大（16）。如果在后来该路由器又从另一个邻居那里接收到一个到达X的有效最小代价，它就用新的最小代价替换无穷大。

HELLO（RFC891）是另一个路由选择向量协议，但它的计量对象是时延，而不是跨度。它起初是为运行在PDP-11处理机上的所谓“Fuzzball”的路由器软件研制的，用以控制继ARPR网之后发展起来的NSFNET。今天，HELLO协议没有被广泛采用，尽管它在发生拥挤的情况下和通过可变链路时有比其它某些协议更好的性能。Hello的一个问题是它所需的同步所有的Hello路由器时钟的机制。这需要一个算法，利用它能在其时延仅可以估算的传输链路上在节点之间传递时间信息。

OSPF（Open Shortest Path First）则是一个现代的链路状态协议，每个网关将它所连接的链路状态信息向其它网关传播。链路状态和路由向量算法之间的差别可以用这样的比喻来说明：路由向量向你的邻居通告整个世界的情况，而链路状态向整个世界通告你的邻居的情况。链路状态机制解决了路由向量产生的许多收剑问题，适用可伸缩的环境。然而，它们是非常强化计算的，典型地需要一台专用机器。OSPF直接运行在IP之上，使用IP分组格式中的协议号89。OSPF分组报文被发送给组播地址224.0.0.5，该地址表示在点到点链路上和广播型多路访问网络上的所有OSPF路由器。在非广播型的网络上需要把OSPF分组发送到具体的IP地址。

6.1.5　互连网控制报文协议

如果一个网关不能为IP分组选择路由，或者不能递交IP分组，或者这个网关测试到某种不正常状态，例如网络拥塞影响IP分组的传递，那么就需要使用互连网控制报文协议（ICMP）来通知源发主机采取措施，避免或纠正这类问题。

ICMP也是在网络层中与IP一起使用的协议。ICMP通常由某个监测到IP分组中错误的站点产生。从技术上说，ICMP是一种差错报告机制，这种机制为网关或目标主机提供一种方法，使它们在遇到差错时能把差错报告给原始报源。例如，如果IP分组无法到达目的地，那么就可能使用ICMP警告分组的发送方：网络、机器或端口不可到达。ICMP也能通知发

送方网络出现拥塞。

ICMP是互连网协议（IP）的一部分，但ICMP是通过IP来发送的。ICMP的使用主要包括下面三种情形：

（1）IP分组不能到达目的地

（2）在接收设备接收IP分组时，缓冲区大小不够。

（3）网关或目标主机通知发送方主机，应该选用较短的路径（如果这种路径确实存在）。

必须懂得，ICMP数据报和IP分组一样，同样不能保证可靠传输。ICMP信息也可能丢失。为了防止ICMP信息无限地连续发送，对ICMP数据报传输的问题不能再使用ICMP传达。另外，对于被划分成报片的IP分组而言，只对偏置等于0的分组片（也就是第1个分组片）才能使用ICMP协议。

为标识ICMP，在IP分组协议段中包含的值是1。重要的是，尽管ICMP报文使用IP协议封装在IP分组中传送，但ICMP不被看成是高层协议的内容，它只是IP中要求的一部分。之所以使用IP递交ICMP报文，是因为这些报文可能要跨过几个物理网络才能够到达最终报宿。因此，ICMP报文不能依靠单个物理网络来递交。

ICMP报文有两种，一种是错误报文，另一种是查询报文。每个ICMP报文的开头都包含三个段：1字节的类型段、1字节的编码段和二字节的检验和段。8位的类型段标识报文，8位的编码段提供关于一个类型的更多信息。16位的检验和的算法与IP头的检验和算法相同，但检查范围限于ICMP报文结构。

6.1.6 可变长子网掩码

术语可变长子网掩码（VLSM:Variable Length Subnet Mask）是指一个网络可以用不同的掩码进行配置。在可变长子网掩码背后的思想是在把一个网络划分成多个子网方面提供更多的灵活性，同时保持在每个子网中能够有足够数量的主机。在没有VLSM的情况下，一个网络只能使用一种子网掩码。这就限制了在给定所需要的子网数目条件下主机的数目。如果你采用的掩码可以具有足够的子网，也许你就不能够在每个子网中分配足够的主机。在另一方面，可以在每个子网中配置足够数量主机的掩码又可能满足不了子网数目的需求。

作为一个例子，假定你被分配一个C类网络号192.214.11.0，并且你需要把网络划分成三个子网，其中一个子网中有100台主机，其余的两个子网各有50台主机。不考虑0和255的特殊性，理论上你有从192.214.11.0 到192.214.11.255的256个可用地址。为了把这256个地址分成多个子网，不使用VLSM，你的一种选择是掩码255.255.255.128，把网络划分成两个子网，每个子网128个地址。另一个选择是255.255.255.192，划分成4个子网，每个子网64个地址。很显然，这两种选择都不能满足你的一个子网中100台主机剩下的每个子网50台主机的要求。使用多重掩码，你可以先用128划分两个子网，每个子网128个地址，然后再把对应第2个子网的地址空间进一步划分成两个子网，每个子网64个地址。

并非所有的路由选择协议都能够处理VLSM。RIP（路由信息协议）第1版和IGRP（内部网关路由协议）在路由更新报文中不运载网络掩码，因此对于使用可变长掩码划分子网的网络不能正确工作。不过现在流行的OSPF（开放的最短通路优先）、EIGRP（增强的内

部网关路由协议）、ISIS（中间系统到中间系统）和RIP第2版等路由协议可以处理可变长掩码。

6.1.7　无类别域间路由选择

无类别域间路由选择（CIDR）的基本思想是以可变大小的方式分配剩下的C类网络地址。比如说，如果一个地方需要2000个地址，那么就分配它一个2048地址的块（8个连续的C类网络），而不是一个完全的B类地址。类似地，一个地方需要8000个地址，就分配给它8192个地址（32个连续的C类网络—8×4× 256）。

除了使用连续的C类网络块作为单位之外，C类地址的分配规则也有所改变。世界被分成4个区域，分配给每个区一部分C类地址空间。具体分配情况如下：

- 欧洲：194.0.0.0——195.255.255.255；
- 北美洲：198.0.0.0——199.255.255.255；
- 中南美洲：200.0.0.0——201.255.255.255；
- 亚洲和太平洋：202.0.0.0——203.255.255.255。

这样，每个区域都分配了大约32×106个地址，另外，从 204.0.0.0到223.255.255.255范围内的大约320×106个C类地址保留作未来使用。这种分配的好处是，现在任何位于欧洲之外的路由器得到一个发往194.xx.yy.zz或者195.xx.yy.zz的分组可以简单地把它传给标准的欧洲网关。在效果上这等同于把32×106个地址压缩成一个路由选择表项。

当然，一旦194.xx.yy.zz分组到了欧洲，就会需要详细的路由表。当一个分组到来时，首先抽出它的目的地址，然后逐项扫描路由选择表，掩码（masking）该目标地址，并将它跟表项比较以寻找匹配。在实践中，路由器的表项往往不是顺次查对，而是使用索引来加快搜索过程。而且有两个表项匹配的情况也是可能的，在这种情况下应该选取其掩码中1位最多的的表项。

6.1.8　移动IP

移动IP的目标是把分组自动地投递给移动结点。一个移动结点是把其连接点从一个网络或子网改变到另一个网络或子网的主机。使用移动IP，一个移动结点可以在不改变其IP地址的情况下改变其驻留位置。

一个移动结点跟一个称作家乡IP地址的固定IP地址相关联。当移动结点在外部网络（即离开家乡网络）的时候，在移动结点的家乡网络上的一个路由器把IP数据报投递给移动结点。该路由器被称作家乡代理。

当一个移动主机出现在外部场点时，它跟那里的外部代理联系，并进行注册。然后外部代理跟用户的家乡代理联系，给它一个关照地址（通常就是外部代理自己的IP地址）。

当发给移动用户的一个IP分组到达用户的家乡LAN时，它在连接到LAN的某个路由器上到达。该路由器用常规的方法确定目的主机的物理地址，即广播一个ARP分组进行询问。家乡代理通过给出自己的MAC地址应答这个ARP请求分组。然后路由器把IP分组发送到家乡代理。

家乡代理把IP分组隧道传送给关照地址，即把该IP分组封装在另一个IP分组的数据段中，后者的目的地址指向外部代理。外部代理收到IP分组后，将其解除封装后把原IP分组包装在数据链路帧中用该网段上的数据链路层地址投递给移动主机。此外，家乡代理还把关照地址发送给IP分组的发送方。随后，发送方可以把后续的IP分组直接隧道传送给外部代理。

6.1.9 IPv6

当前采用的IP协议是它的第4版（IPv4），IPv5的称号被赋给了一个实验的称为流协议的面向连接的互连网协议。现在人们普遍意识到，IPv4的剩余生命期已经屈指可数了，并且最终要被一个称为IPv6的新协议替代。

1990年，Internet 工程任务组（IETF）就着于研制一个新的IP版本，其主要目标如下：

（1）具有非常大的地址空间，即使各个单位和组织对分配的地址利用率不高，也能支持数十亿以上的主机。

（2）减少路由选择表的尺寸。

（3）简化协议，允许路由器更快地处理分组。

（4）提供比现在的IP更好的安全性（身份验证和保密）。

（5）更多地关注服务类型，特别是实时数据。

（6）通过允许指定范围来辅助组播服务。

（7）允许主机移动地理位置（漫游）而不用改变其IP地址。

（8）允许协议在未来进一步演变。

（9）允许老的和新的协议在若干年内共存。

1992年6月IETF公开征求对下一代IP（IPng）的建议，随后收到了若干个提案，到1994年就形成了Ipng的最后设计。1995年1月RFC 1752“下一代IP建议书”的发表是一个重要的里程碑。RFC1752概述了IPng 的需求，规定了PDU格式，突出了下一代IP在寻址、路由选择和保安等方面采用的方法。这个新一代的IP现在已正式地称作IPv6。有一系列的Internet文档描述IPv6的细节，它们包括从总体上描述IPv6的RFC1883，讨论在IPv6头中的流标记的RFC1809，以及处理IPv6寻址方面的RFC 1884、RFC1886和RFC1887。

虽然IPv6跟IPv4不兼容，但是总的来说它跟所有其它的Internet 协议兼容，包括TCP、UDP、ICMP、IGMP（Internet组管理协议）、OSPF、BGP（边界网关协议）和DNS（域名系统），只是在少数地方作了必要的修改（大部分是为了处理长的地址）。IPv6相当好地满足了预定的目标。首先也是重要的，IPv6有比IPv4长得多的地址。IPv6的地址用16个字节表示，地址空间是IPv4的296倍，相当于地球表面的每平方米面积都有大约6×1023个具唯一性的地址。无论未来怎样发展，看来这么多的地址也是够用的。

IPv6第二个主要的改进是简化了IP分组头，它包含8个段（IPv4是12个段）。这一改变使得路由器能够更快地处理分组，从而可以改善吞吐率。

第三个主要改进是IPv6更好地支持选项。这一改变对新的分组头很重要，因为一些从前是必要的段现在变成可选的了。此外，表示选项的方式也有所不同，使得路由器能够简

单地跳过跟它们无关的选项。这一特征加快了分组处理速度。

IPv6有重大举措的第四个方面是安全性。身份验证和保安功能是这个新的IP的关键特征。

最后一项重要改进是有关资源分配的。取代IPv4的服务类型段，IPv6的流标记段支持对属于一个特别的交通流（对应的发送端可能请求特别的处理）的标记，从而能够支持诸如实时视频这样的特殊交通。

如图6-1所示，IPv6分组头有固定的40字节长度，由下列段组成：

- 版号（4位）：IP协议版本号，其值为6。
- 类别（8位）：包含优先级值和4个保留位。
- 流标记（20位）：可以被主机用来标记请求在网络内的路由器对其进行特别处理的那些分组。
- 载荷长度（16位）：以字节计的紧随IPv6头的IPv6分组剩余部分的长度。也就是说，这是所有扩展头再加上传输层PDU的总长度。
- 下一个头的类型（8位）：标识紧随该IPv6头的头的类型。注意，IPv6头和每一个扩展头都包括一个“下一个头的类型”段，这个段标识紧随其后的头类型。如果下一个头是一个扩展头，那么这一段包含那个头类型标识，否则这个段包含使用IPv6的高层协议的标识（典型地是一种运输层协议），使用跟IPv4的协议（Protocol）段相同的值。
- 跳段限制（8位）：允许该分组跨越的剩余跳段数。跳段限制段被源设置成所希望的最大值，随后被转发该分组的每个节点减值1。如果跳段限制被减值至零，那么该分组就要被丢弃。这要比IPv4的生存时间段所需要的处理简单；

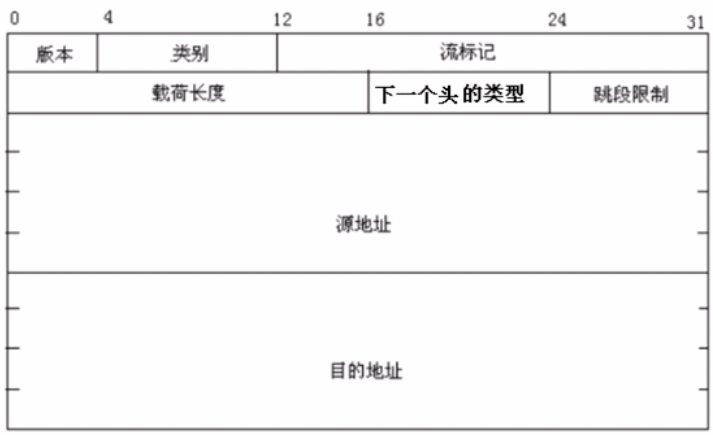


图 6-2　IPv6 分组的固定头

- 源地址（128位）：发送该分组的源计算机的地址；
- 目的地地址（128位）：将要接收该分组的接收方计算机的地址。事实上，如果存在路由选择头，这可能不是最终目的地地址。

虽然IPv6头较之IPv4头的必要部分要长（40字节对20字节），但包含较少的段（8对12），

因此路由器为每个头所做的处理较少，从而加快了路由选择。

IPv6标准建议在使用多个扩展头时，IPv6的头以下列次序出现：

（1）IPv6头，必需的头，总是出现在开头位置。

（2）按跳段逐级处理的选项头。

（3）目的地选项头，用于被在IPv6目的地址段中出现的第一个目的地处理（例如由源路由选择规定的第1个目的路由器地址）的选项，这些选项也会被随后在路由选择头中列出的目的地（例如由源路由选择规定的其它路由器地址）处理。

（4）路由选择头。　（5）分割头。　（6）身份验证头。

（7）加密安全性载荷头。

（8）目的地选项头：用于仅被分组的最终目的地处理的选项。

6.1.10　组播

为了能够支持像视频点播和视频会议这样的多媒体应用，网络必须实施某种有效的组播（也称多播或组播）机制。使用许多个单投点传送来仿真组播总是可能的，但这会引起主机上大量的处理开销和网络上太多的交通量。我们所需要的组播机制是让源计算机一次发送的单个分组可以抵达用一个组地址标识的若干台目标主机，并被它们正确接收。

使用组播的缘由是有的应用程序要把一个分组发送给多个目的地主机。不是让源主机给每一个目的地主机都发送一个单独的分组，而是让源主机把单个分组发送给一个组播地址，该组播地址标识一组主机。网络（比如Internet）把这个分组给该组中的每一个主机都投递一个拷贝。主机可以选择加入或离开一个组，而且一个主机可以同时属于多个组。

在Internet中的IP组播也使用组播组的概念，每个组都有一个特别分配的地址，要给该组发送的计算机将使用这个地址作为分组的目标地址。在IPv4中，这些地址在D类地址空间中分配，而IPv6也有一部分地址空间保留给组播组。主机使用一个称作IGMP（Internet组管理协议）的协议加入组播组。它们使用该协议通知在本地网络上的路由器关于要接收发送给某个组播组的分组的愿望。

通过扩展路由器的路由选择和转发功能，我们可以在许多由路由器互连的支持硬件组播的网络上面实现Internet组播。

在链路状态路由选择中，每个路由器监视跟它直接相连的链路的状态，当状态改变时，就给所有其它的路由器发送一个更新报文。由于每个路由器都收到了可以重构整个网络拓扑的足够信息，所以它们都能够使用Dijkstra算法计算以自己为根到达所有可能的目标的最短通路分布树。路由器使用这个树确定它转发的每个分组的下一跳段。

为了支持组播，我们对上述算法所做的扩展就是把在一个特别的链路（LAN）上具有成员的若干个组加到该链路的状态上。惟一的问题是每个路由器如何确定哪个组在哪个链路上有成员。答案是让每个主机定期地向LAN通告它所属于的组。路由器只须监视LAN以得到这样的通告。如果这样的通告停止到达了，那么在一段时间之后路由器就认为该主机已经脱离了这个组。

如果具备了哪个组在哪个链路上有成员的完全信息，那么每个路由器都能够使用Dijkstra算法计算任一源到任一组的最短通路组播树。每个路由器必须潜在地为从每个路由

器到每个组都保持一个单独的最短通路组播树。这显然是很昂贵的举措，因此取而代之的是，路由器只是计算和存储这些树的一个高速缓存，只为当前处于活动状态的每个源/组对缓存一个最小通路组播树。

把组播加到距离向量算法上要稍微复杂一些，因为路由器不知道互联网络的整个拓扑结构。每个路由器维持一张由若干个“目的地，代价，下一跳段〉组成的表，并且与它直接相邻的节点交换由若干个“目的地，代价”对组成的列表。把该算法扩展成支持组播是包括两个阶段的过程。首先，需要设计一个广播机制，允许把分组转发到互联网上的所有网络。第二，需要优化这个机制，以便它剪除没有属于该组播组的主机的网络。

每个路由器都知道通过“下一跳段”到达一个指定目的地的当前最短通路。因此，每当它接收到一个来自源S的组播分组时，如果当并且仅当该分组是在前往S的最短通路上的链路上到达的，也就是说，分组来自在路由表中跟S相关联的下一跳段，那么它就把分组在所有的外出链路上转发（分组由其到达的那条链路除外）。这一策略有效地把分组从S向外洪泛，但不会把分组回送给S。

当多个路由器连接到一个给定的LAN时，应该删除所产生的重复广播分组。一种举措是对于一个源在每条链路（LAN）上把一个路由器指定为父路由器，仅仅父路由器可以在该LAN上转发组播分组。具有到达源最短通路的路由器被选作父路由器。如果两个路由器到达源的距离相同，则选取具有最小地址的路由器。一个路由器可以根据它与它的邻居交换的距离向量报文知道它是否是所连接的LAN的父路由器（相对于每个可能的源）。

值得注意的是，这种优化需要每个路由器（相对于每个源）为它的每个输入链路用1个比特表示它是否是那个源/链路对的父亲。事实上，在互联网络上，一个源是一个网络，而不是一台主机，因为互联网路由器只对在网络之间转发分组感兴趣。这样所产生的机制有时称作反向通路广播（RPB）。

反向通路广播（RPB）实现最短通路广播，但需要进行修剪操作，留下接收前往组G的每个分组的网络，去除其中没有组G的成员的主机的网络。

协议无关的组播（PIM）是针对业已存在的组播路由选择协议的可扩展性问题提出来的。特别是，人们已经认识到，在只有小部分的路由器想要接收发给某个组的交通量的环境中，现有的协议的扩展性不是很好的。例如，如果大部分路由器都不要接收这类交通，那么在它们被明确地从发送目标中删除以前一直广播给所有的路由器的做法不是一个好的设计。这种情况的存在是如此地普遍，以至于PIM把问题划分为“稀疏方式”和“密集方式”两个空间。由于现有协议对稀疏环境的适应性很差，所以PIM的稀疏方式得到了人们普遍的关注。

在PIM稀疏方式（PIM-SM）中，路由器使用称作加入和修剪报文的PIM协议报文明确地加入和脱离组播组。问题在于往什么地方发送这些报文。为此，PIM为每个组指定一个会合点（RP）。在一个域中的若干个路由器被配置成侯选会合点。PIM定义了一组规程，让在域中的所有路由器都认同把某个路由器用作会合点。这些规程是相当复杂的，因为它们必须处理广泛的细节问题，比如说，一个侯选会合点的失效，以及由于若干链路或节点的失效把一个域分割成两个互相隔离的网络等。

PIM是跟单投点路由选择协议无关的，也就是说，它不限于某一个路由选择协议。这主要是相对于其它的组播路由选择协议而言，后者是源于链路状态或距离向量路由选择。

不过，PIM在很大程度上是跟Internet协议捆绑在一起的，所以就网络层而言，它又不是协议无关的。

6.1.11 集成服务和差分服务

现有的提供QoS的方法可以分成两个广泛的类型：

- 精细方法。可为具体的应用或信息流提供QoS；
- 粗旷方法。为大类数据或聚合交通提供QoS。

在第一个类别中有集成服务，它是由IETF提出的一个QoS体系结构，通常跟RSVP（资源预留协议）相关联。在第二个类别中有“区分服务”，也是由IETF提出的标准。集成服务主要针对单个流的特征类型来描述QoS，后者则通过聚集流的特征类型来描述QoS。由此可以看出，一个是要求端系统和中间节点共同参与的控制，另一个则将改进集中在核心网络。

RSVP相对于区分服务来说，颗粒度更细、更复杂，要求也更高，通常不易在核心网上实现。端系统可以用RSVP请求较细粒度的QoS控制参数，在骨干网边界路由器的进入点将这些预留请求影射成由DS（区分服务）字段指示的服务级别，在骨干网的出口，再将RSVP参数还原给最终目的地。

区分服务模型是对少量种类的交通分配资源。事实上，区分服务的一些方法就是简单地把交通划分成两个类别。考虑到网络运营者在试图保持尽力而为的互联网能够平滑运营时所经历的困难，只把少量的新机制加进原有的服务模型显然是很有意义的。

IETF的区分服务工作组标准化了适用于标记分组的路由器行为。这些行为被称作每跳段行为（PHB），该术语表示他们所定义的是具体的路由器的行为，而不是端到端的服务。因为有不止1个的新行为，所以有必要在分组头中使用多于1个的位来告诉路由器采用哪一个行为。IETF决定利用IP头中的TOS（服务类型）字节，该字节已经被广泛使用，现在对它进行重新定义。他们把这个字节中的6位值分配给区分服务码点（DSCP），每个DSCP都是一个6位值，标识可用于分组的一个特别的PHB（每跳段行为）。

6.1.12 多协议标记交换

多协议标记交换（MPLS）的出现源于早期的IP交换解决方案，因此它的体系结构是基于已经提出的IP交换的思想、概念和组成部件。它的基本目标之一是简化通过网络转发IP分组的过程。在传统的IP转发机制中，每个路由器都要分析包含在每个分组头中的信息，提取目标地址，执行基于目标地址的路由表查询，以及计算头检验码、减少TTL（存活时间）的值和完成合适的出口链路层封装。有效的业务流转发不仅依赖于路由器自身的功能，而且要依赖于路由信息交换协议（即路由选择协议）来计算最佳的下一跳。或者简单地说，每个路由器处理每个分组的过程都是：分析分组的网络层的头字段，根据目标地址前缀为分组分配一个FEC（转发等效类），然后将FEC映射到下一跳路由器。

在MPLS网络中，入口路由器不是将FEC映射到下一跳路由器，而是在分组上添加表示它所归属的FEC的一个标记。在下一跳路由器上，因为分组已经跟FEC相关联，所以没有

必要再检查网络层的头。标记被用来索引一个包含输出端口和一个新标记的连接表项。旧标记被新标记取代，然后分组被从输出端口转发到下一跳路由器。

标记交换的一个重要的结构特征是把基于标记的转发操作从网络层的控制功能中分离出来，使得网络运营者能够把若干当前和未来的业务与一组标记相关联。MPLS网络的入口路由器可以把分组映射到不同FEC的任何编号上。例如，一个FEC可能基于目的地选路、组播（即多投点）选路、一个源端/目的端地址对、一个源地址或者甚至是网络入口的物理点。一个FEC也可以表示所有经过一个显式的非缺省路径的分组。无论为分组分配FEC的机制多么复杂，网络对分组的转发仍然是基于标记交换。与传统的IP转发机制相比，MPLS使得基于策略的选路以一种更简单的更直接的方式进行。这样，如果需要引入新的网络层控制功能，就可以不必重新优化或升级转发通路上的组件和设备。当发生不可预见的必要的网络层变化时，已有的投资可以得到保护。例如，当需要引入IPv6以获得更大的地址空间时，不需要对现有的转发通路做任何实质性的修改。

MPLS的实质是将路由器移到网络的边缘，将快速、简单的交换机置于网络主干，对一个连接请求实现一次路由选择，多次交换。其主要目的是将标记交换转发数据报的基本技术与网络路由选择有机地集成。

因为MPLS头不是网络层分组的部分，也不是数据链路层帧的部分，所以它在很大程度上是独立于这两个层次的。这一特征意味着，我们可以建立一个MPLS交换机，它既能够转发IP分组，也能够转发ATM信元，输入的是哪种PDU ,就转发哪种PDU。这一特征也正是在MPLS名称中“多协议”的来源。

6.2　基本练习题

1．填空

选择发送IP分组的通路的过程被称作_____。

解答：选择发送IP分组的通路的过程被称作__路由选择__。

2. 填空

IPv6允许三种类型的地址，它们分别是（1）_____地址（2）_____地址（3）_____地址。

解答：IPv6允许三种类型的地址，它们分别是（1）_____单播_____地址（2）____任播___地址（3）_____组播____地址。

3. 假定你在北京有一台PC，在上海有另一台PC。不计由电信部门提供的任何设备，那么连接这两台PC最少需要多少个部件？

解答：4个。使用一条CAT5交叉电缆把在北京的PC连接到一台路由器，再使用一条CAT5交叉电缆把在上海的PC连接到放在那里的一台路由器。如图6-3所示，最后把两台路由器用由电信部门提供的长途线路互连。

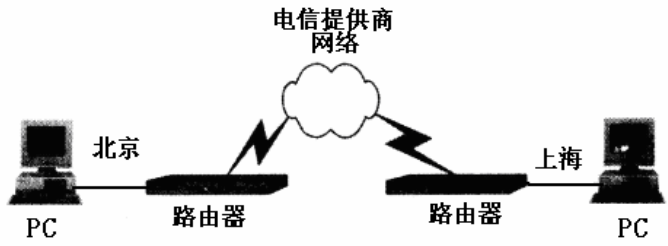


图 6-3　通过路由器互连的网络

4. 假定一台计算机使用的网卡是标注AUI的15针连接器，而集线器只有RJ-45插口。你应该怎样把它们连接起来？

解答：虽然大多数的网卡都有一个RJ-45插口，但AUI端口允许更大的灵活性。可以把一个叫做收发器的设备附接到该AUI端口，收发器的另一端可以是一个RJ-45插口。事实上，收发器可以有许多类型的插口，除AUI和RJ-45外，还有细缆以太网插口和光缆插口。这就允许管理员使用不同类型的以太网，包括10Base-T、10Base2、10Base5和10Base-F。所有这些都不用改变在计算机中的网卡，也不用改变软件驱动程序。因此，本题的答案是把一个另一端带有一个RJ-45插口的收发器连接到网卡的AUI端口，并且使用1根正常的CAT5电缆把该收发器连接到集线器。

5. 使用以太网技术连接两台PC所需要的最小数量的部件是什么？

解答：总共3个部件：这两台PC和一条交叉连接电缆。CAT5交叉电缆连接到每一台PC中的网卡（NIC）。交叉电缆在所有方面都跟正常的电缆相同，但把导线的发送对和接收对颠倒，使得一台PC发送的信号在正确的导线上被另一台PC接收。如果使用正常的电缆，一台PC将会把信号发送到第二台PC上的Tx（发送）导线，结果会被第二台PC忽略。图6-4示出了上述交叉电缆对两台PC的连接。由于集线器（hub）端口具有内建的交叉，因此正常的电缆可以直接通过。

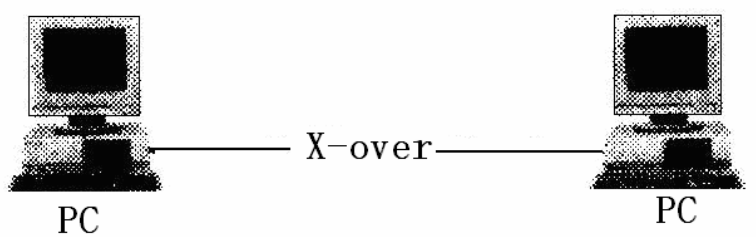


图 6-4　两台 PC 通过交叉电缆的连接

6. 如果在某城市的另一端的办公室里还有3台PC，那么把本办公场点的设备跟那3台PC互连的最常用的方法是什么？

解答：在远程场点3台PC处放置另一个集线器（Hub），并用3条CAT5电缆把那3台PC连接到该集线器。再在该集线器处安装一台带有一个以太网接口的路由器，并用另1条CAT5电缆把路由器也连接到该集线器。类似地，在本地场点也安装一台路由器，并用1条CAT5

电缆连接到本地集线器。最后，再通过由电信部门提供的一条线路（例如一条ISDN链路或T1线路）把这两台路由器互连。

7. 假定在本地办公场点有一个由10台PC组成的网络。其中有5台PC连接到一个以太网集线器（Hub），其余5台PC连接到另一个以太网集线器。这两台集线器都连接到一个局域网交换机。一台路由器把本地场点的这个交换机连接到具有相同配制的一个远程办公室。那么，本地场点的LAN交换机能够获悉多少个MAC地址？

解答：本地交换机能够获悉所有10台PC的MAC地址，加上本地路由器的MAC地址，总共11个MAC地址。集线器不是第2层设备，因此它们没有MAC地址。而且本地LAN交换机仅在本地网络上运行，因此它不知道在本地路由器另一侧的任何MAC地址。

8. 假定你正在使用一个在以太网上的工作站访问在Internet上的一个Web场点。使用一个网络监视器或分析仪，你怎样能够查得你的机器的网卡的硬件地址？

解答：为了确定在以太网上的工作站的地址，需要从媒体捕获正在被传输的来自该工作站的分组。一旦这样的分组被捕获到了，检查以太网帧的头部的源地址段就能揭示出该工作站网卡的硬件地址。

9. 把LAN交换机跟集线器（hub）和路由器结合使用的优点是什么？

答：把像是服务器这样的设备连接到LAN交换机上一个专用的端口可以避免来自连到同一网段上的其它设备的交通。用hub连接的设备会看到连到同一hub上的其它设备发出的交通。但如果把hub连接到一个LAN交换机，那么在该hub上的设备将不会看到连到同一LAN交换机的其它hub上的交通。路由器用来把一个网络连接到另一个网络。路由器隔离广播。由于LAN交换机不处理网络层分组，所以从一个网络到达另一个网络（例如从一个IP子网到另一个IP子网）需要使用路由器。

10. 假定你怀疑连接两台设备的单模光缆有问题。你的朋友建议你拔出光缆的一端，并且往它里面看，判断是否仍在发送光。从下面列出的4项中选择两项来评述这一建议。

a. 这是一个好主意，因为你可以搞清楚另一个设备是否在发送光。
b. 这是一个坏主意，因为激光不使用可见光谱中的频率。
c. 这是一个坏主意，因为激光会烧坏你的视网膜。
d. 可以，激光没有那么强，对你不会有伤害。

解答：a和c。假定设备仍在发送光，那么你可以看到光，但你会失去视力。因此这是一个很坏的建议。任何时候都不要往光缆或任何种类的激光里面看，而不管它是否是可见光。

11. 网络拓扑的选择需要考虑哪些因素？

解答：许多年以前，考虑的主要因素是PC和服务器的物理安排，需要多大带宽，以及在网上最常传输的交通图案的种类。然而现代局域网几乎全部是以太网，它是一种星形拓扑。它在很大程度上是因为大多数企业也需要电话，同时敷设电话和数据电缆是容易的。

事实上，它们通常使用相同的电缆。这种拓扑也跟成本和可提供性有关，因为几乎没有竞争。在广域网上，考虑的因素通常是成本，因为维持数据电路的每月费用可能是很昂贵的。因此，尽管从技术角度出发，在远程办公室之间的ATM或帧中继全网状拓扑可能是有益的，但在财务开销方面却很难被证明是合理的。随着网络的演变，在广域网中星形拓扑也逐步流行起来。这种情况始于小公司，它们需要把两个场点连接在一起，配制点到点的网络。当公司发展壮大时，增加场点，增加点到点的线路。这些线路通常是从公司总部连到各个远程的分公司场点，产生一种星形结构。

12. 试说明LAN交换机过滤和转发分组所使用的地址类型。

答：在局域网上，LAN交换机运行在数据链路层的MAC子层，并且使用MAC地址信息。LAN交换机不知道数据分组的网络层PDU是IP、IPX，还是其它什么类型；LAN交换机把所有的分组都同等对待。

13. 下列协议中的哪一个使用等级式编址或命名结构？

（a）DNS　（b）ARP　（c）BOOTP　（d）LDAP（轻量级目录访问协议）

解答：a 和d。域名服务（DNS）使用等级式名字结构表示在一个TCP/IP网络上设备的名字。使用等级式名字结构的TCP/IP协议的另一个例子是轻量级目录访问协议（LDAP）。

14. 一个设备怎样识别一个输入分组是ARP请求？

解答：在一个ARP请求分组中，帧类型段是十六进制值0x0806。因此，当该设备察看一个输入分组时，帧类型0x0806表明该分组是一个ARP请求。

15. 一个ARP广播请求的发送方期待接收多少个响应？

解答：ARP请求报文的发送方仅期待接收一个响应，因为仅仅一个设备应该具有在ARP请求分组中说明的IP地址。

16. 术语多归宿的含义是什么？

解答：在一个IP网络上，对网络有多于一个的接口或连接的设备叫做多归宿系统（multi-homed system）。

17. 对于一个D类IP地址，第1个字节的预留位图案是什么？

解答：一个D类地址的第1个字节的位图案是：1110xxxx。

18. 总共可能有多少个B类网络？

解答：对于B类地址，可以用于网络部分的位的个数是14，其中6位来自第1个字节，8位来自第2个字节。把2^{14}转换成十进制得到16384。因此在IP地址空间中最多有16 384个B类网络。

19. 在一个对于IP地址为192.168.44.64的设备的ARP请求分组中目标地址是什么？

解答：FF-FF-FF-FF-FF-FF。因为发送方不知道目标设备的物理地址，所以发送一个广

播分组，目标硬件地址段用全1表示。

20. 你认为可以重新设计当前的IP编址方案，使用设备的硬件地址代替IP号码吗？请解释你的答案。

解答：不可以。因为在硬件地址中没有等级结构，地址中没有对所有设备都通用的共用部分。由于MAC地址没有共用部分来鉴别设备驻留在哪个网段上，路由选择表必须包括所有设备的地址。这将使得路由表变得非常大和不可管理。

21. 为了提供更多的子网，为一个B类地址指定了子网掩码255.255.240.0。每个子网可以有多少台主机？

解答：4094台主机。子网掩码使用在第三字节中的前4位建立子网，将255.255.240.0用二进制表示是：

11111111.11111111.11110000.00000000

因此有12位可用于主机地址，

主机数=2^{12}-2=4094

22. 在上题中，总共可以有多少个子网？

解答：14个子网。子网掩码255.255.240.0使用在第三字节中的前4位建立子网，

所以，子网数=2^4-2=14。

23. 一个单位要在4个子网上使用专有的网络号192.168.90.0。在每个子网上最多配备25台主机。该单位应该使用什么样的子网掩码？

解答：255.255.255.192。要为网络192.168.90.0建立4个子网，至少要把主机地址部分的前3位用于建立子网。这样，子网数=2^3-2=6。同时要考虑每个子网至少支持25台主机的条件，若用其余的5位主机地址，可以支持的每个子网内的主机数等于2^5-2=30。

24. 无类别地址192.168.10.0/20所使用的具体IP地址是什么？

解答：192.168.10.0/20表示一个连续的C类地址块，每个地址的前20位相同（前两个字节是192.168，第三字节位图案是0000xxxx），而且是固定值。就第3字节而言，地址块的起始值是10（十进制），即二进制00001010。下面列出相继的第3字节的值：

十进制	第3字节的二进制表示
192.168.10.0	00001010
192.168.11.0	00001011
192.168.12.0	00001100
192.168.13.0	00001101
192.168.14.0	00001110
192.168.15.0	00001111

因此，192.168.10.0/20所对应的IP地址范围是192.168.10.0到192.168.15.0。

25. 在地址解析中网关可以起什么作用？

解答：在地址解析中网关可以起到代理ARP的作用。代理ARP基于网关作为远方主机代理的概念，它适用于为将IP地址映射成物理网络地址而采用ARP或类似方法的任何广播网络。作为例子，假定IP子网地址为IPN1的以太网上有一台IP地址为IPH1的主机。它要发送一个分组给另一个以太网（IP子网地址为IPN2）上IP地址为IPH2的主机。连接这两个子网（以太网）的网关G具有两个以太网地址：ETN1G和ETN2G。现在假定计算机IPH1发送一个关于计算机IPH2的ARP请求分组。计算机IPH2不能回答这一请求，因为它在另一个子网上，收不到这一请求。然而网关G可以代表计算机IPH2回答请求。当IPH1说：“地址是IPH2的主机，请告诉我，你的以太网地址是什么？”网关G回答：“我在这里，我的IP地址是IPH2，以太网地址是ETN1G。”不过，这里的ETN1G并不是计算机IPH2的以太网地址，而是网关G的一个以太网地址。这样计算机IPH1认为IPH2直接连在本地以太网上，其硬件地址是ETN1G。尽管这不是事实，但却能解决问题。每当有一个IP分组要发往IPH2，计算机IPH1都将它送给以太网地址ETN1G。由于这是网关G的以太网地址，网关G得到IP分组。然后网关G再将分组传往目的地。

26. 子网掩码的目的是什么？

解答：当一个分组到达一个路由器时，路由器需要能够确定IP地址的网络部分。子网掩码被用来确定IP地址的哪个部分是网络部分，哪个部分是主机地址。为了完成这种号码分离，路由器执行IP地址跟子网掩码的AND操作，就能得到它的网络部分。

27. 什么是组播？

解答：D类IP地址就是为组播保留的。组播提供把一个报文发送给一组设备的能力，这组设备都是同一个组播组的成员。

28. 试解释地址解析的封闭计算方法。

解答：在封闭形式的计算方法中，选择每个设备使用的软件地址，使得物理地址可以通过某种形式的数学计算推导出来。这种地址解析方法在可以设定设备的物理地址的环境中工作得很好。有了这一功能，管理员就可以建立一个物理的和软件的编址方案，使得从软件地址到物理地址翻译的工作量最小，且速度快。

29．针对一台通过以太网集线器连到TCP/IP网络的Unix主机，回答下列问题：

（1）什么命令使用地址分辨协议（ARP）决定一台远方主机的以太网地址？
（2）什么命令使用ICMP协议得到网上一台远方主机的响应？
（3）什么命令显示网络状态？
（4）什么命令可以设置跟主机的一个网络接口相关的选项和参数？

解答：（1）arp
（2）ping
（3）netstat
（4）ifconfig

30．在一台连接到TCP/IP网络的Unix主机上可以使用什么命令和守护程序来操纵路由

选择信息？

解答：route 命令和routed守护程序。

31．通常，Unix主机的名字和IP地址都可以在哪个文件中找到？

解答：/etc/hosts文件。

32．计算机little-sister.cs.vu.nl的IP地址是130.37.62.23，那么该计算机是在A类、B类还是C类网上？

解答：由于该计算机IP地址的开头8位是十进制数130，因此它是在B类网络上。

6.3　综合应用练习题

1．如图6-5所示，一台路由器连接三个以太网。请根据图中给出的参数解答下列问题：

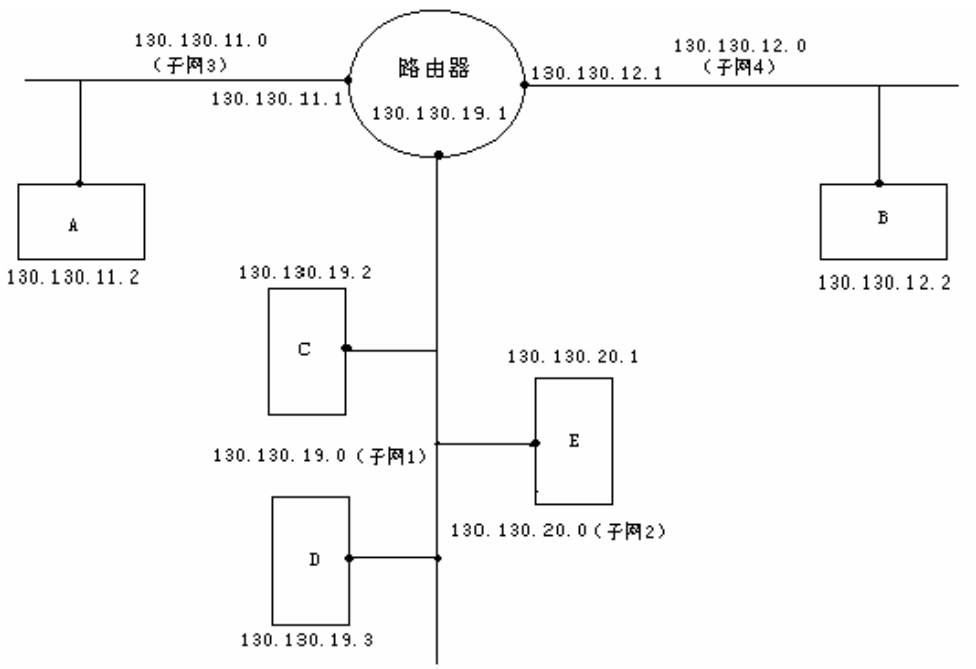


图 6-5　习题 1 插图

（1）该TCP/IP网络使用的是哪一类IP地址？

（2）写出该网络划分子网后所采用的子网掩码。

（3）系统管理员将计算机D和E按照图中所示结构连入网络并使用所分配的地址对TCP/IP软件进行常规配置后，发现这两台机器上的网络应用程序不能够正常通信。这是为什么？

（4）假定主机C运行Berkeley UNIX操作系统，那么在主机C上你将使用什么命令去告

诉网络软件子网130.130.20.0和子网130.130.19.0是在同一以太网上？

（5）如果你在主机C上要发送一个IP分组，使得主机D和主机E都会接收它，而子网3和子网4上的主机都不会接收它，那么该IP分组应该填写什么样的目标IP地址？

解答：（1）该TCP/IP网络使用的是B类IP地址

（2）该网络划分子网后所采用的子网掩码是255.255.255.0

（3）这两台机器上的网络应用程序不能够正常通信，那是因为在一个以太网上不能使用不同的子网号。在这种配置情况下，IP软件会试图将IP分组送往网关，而不会直接投递。最终，IP分组将会被该网关丢弃。

（4）# route　add　130.130.20.0　130.130.19.1　0

（5）255.255.255.255

2. 一台以太网主机加入多播组225.128.47.81，具有什么样的MAC地址的一个帧的到达将引起网络接口卡（NIC）中断CPU？

解答：01-00-5E-00-2F-51。以太网地址长度是6个字节，第1位表示是单地址（0）还是组地址（1）。全局唯一的地址由IEEE以地址块的形式分配给各个团体。在以太网的地址格式中，开头24位表示团体的唯一标识，地址块内地址分配的唯一性则由制造厂商保证。为了把IP多播地址映射到以太网的多播地址，只需要把IP组播地址的低序23位放入特别的以太网多播地址01.00.5E.00.00.00（16进制）的低序23位即可。IP多播地址225.128.47.81（十进制点分表示）的低序24位是128.47.81，81的十六进制表示是51，47的十六进制表示是2F，字节128用二进制形式表示是1000 0000，所以其后面7位是000 0000，再在前面加上一个0（来自以太网多播地址01.00.5E.00.00.00左数第4字节中的第1个0）就是0000 0000，用十六进制表示就是00。因此具有01-00-5E-00-2F-51 MAC地址的一个帧的到达将引起网络接口卡（NIC）中断CPU。

3. 另一台以太网主机加入多播组255.128.47.81，具有什么样的MAC地址的一个帧的到达将引起网络接口卡（NIC）中断CPU？

解答：01-00-5E-01-2F-51。第1个字节的第1位总是1，开头3个字节总是01.00.5E。把IP地址的最后23位转换成十六进制就得到答案，即从1.47.81得到01-2F-51，再把01-2F-51附加到01.00.5E的后面就得到01-00-5E-01-2F-51。因此具有01-00-5E-01-2F-51 MAC地址的一个帧的到达将引起网络接口卡（NIC）中断CPU。

4. IP网络192.168.130.0使用子网掩码255.255.255.224，下列主机在什么子网上？

192.168.130.10　192.168.130.67　192.168.130.93　192.168.130.199
192.168.130.222　192.168.130.250

解答：子网掩码255.255.255.224的第4字节用二进制表示是11100000，使用主机号部分3位划分子网。可能的子网数是2^3-2=6，每个子网内主机的最大数目是2^5-2=30。各个子网内主机地址的分布情况如下：

子网的网络号　　可能的主机地址范围

192.168.130.32	33--62
192.168.130.64	65--94
192.168.130.96	97--126
192.168.130.128	129—158
192.168.130.160	161—190
192.168.130.192	193--222

显然，IP地址192.168.130.10和192.168.130.250不可能在使用子网掩码255.255.255.224的192.168.130.0的网络上使用。IP地址192.168.130.67和192.168.130.93在子网64上，IP地址192.168.130.199和192.168.130.222在子网192上。

5．通常，当一个移动主机不在居所的时候，送往它的居所LAN的分组被它的居所代理（home agent）截获。对于一个在802.3 LAN上的IP网络，居所代理如何完成这个截获任务？

解答：可以想到的一种方法是让居所代理不加选择地读在LAN上传送的所有帧，通过察看其中的IP地址确定是否指向移动主机。该方法的缺点是效率非常低。通常采用的替代方法是通过响应ARP请求，居所代理让路由器认为它（指居所代理）就是移动主机。当路由器得到一个前往移动主机的IP分组时，它广播一个ARP查询请求，询问与目的地计算机（即移动主机）的IP地址相对应的802.3 MAC级地址。当移动主机不在居所时，居所代理响应该ARP请求，从而路由器把移动用户的IP地址跟居所代理的802.3 MAC 级地址相关联。

6．有一个使用“严格源路由选择”选项的IP数据报必须被分割传送。你认为是要把该选项拷贝到每一个分割的片段，还是仅拷贝到分割后的第一个片段就可以了呢？请解释你的答案。

解答：因为为每一个分割的片段选择路由都需要该选项信息，因此该选项必须出现在每一个片段中。

7. 假定IP的B类地址不是使用16位而是使用20位作为B类地址的网络号部分，那么将会有多少个B类网络？

解答：除去2位作为前缀，将剩下18位表示网络。从概念上讲，网络数目可以有2^{18}或262144个。然而，全0和全1是特别地址，所以只有262142个可提供分配。

8. 试把以十六进制表示成C22F1582的IP地址转化成点分十进制表示。

解答：用点分十进制表示，该IP地址是194.47.21.130。

9．有人说，“ARP向网络层提供服务，因此它是数据链路层的一部分。”你认为他的这种说法对吗？

解答：不对。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。

10．ARP和RARP都把地址从一个空间影射到另一个空间。在这方面，它们是相似的。

然而，它们的实现是根本不同的。试问，它们的不同点主要表现在什么方面？

解答：在RARP的实现中有一个RARP服务器负责回答查询请求。在ARP的实现中没有这样的服务器，主机自己回答ARP查询。

11．给出一种在目的地重组IP片段的方法。

解答：一般情况下，片段可能不是按照顺序到达，有的也可能在途中丢失。而且，在最后一个片段到达之前，不知道被分割的IP数据报的总长度。也许处理重组的唯一方法是缓存所有的片段，直到最后一个片段的到达，知道IP数据报的尺寸。建立一个适当大小的缓冲区，把各个片段都放进缓冲区，同时维持一个位图，用8个字节1比特保持跟踪哪些字节已经存放在缓冲区中。当位图中的所有比特都是1时，表示该IP数据报是完整的。

12．大多数IP数据报重组算法都有一个计数器来避免一个丢失的片段长期挂起一个重组缓冲区。假定一个数据报被分割成4个片段。开头3个片段到达了，但最后一个被耽搁了，最终计数器超时，在接收方存储器中的3个片段被丢弃。过了一段时间，最后一个片段蹒跚而至。那么应该如何处置这个片段？

解答：对接收方而言，这是一个新的IP数据报的一部分，该数据报的其它部分还不得而知。收到的这个片段被放在队列中，等待其余片段的到来。显然，在其余片段不可能到达的情况下，这个片段最终也会因超时而被丢弃。

13．一个路由器在其路由表中具有下列路由：

路由	输出接口
0.0.0.0 /0	e1
10.0.0.0 /8	e0
10.0.0.0 /16	e1
10.0.1.0 /24	s0
10.1.1.0 /24	s1
10.1.0.0 /16	s0
10.1.0.0 /24	e1
10.1.1.1 /32	s2

一个目标地址是10.1.1.1的分组到达该路由器，该路由器将使用哪个接口转发该分组？

解答：s2。不管路由表中的路由是按照怎样的顺序排列的，路由器总是取最长匹配。在这里，由于/32是最长最具体的匹配，因此将使用它的外出接口s2。

14．一个路由器在其路由表中具有下列路由：

路由	输出接口
0.0.0.0 /0	e1
10.0.0.0 /8	e0
10.0.0.0 /16	e1

10.0.1.0 /24	s0
10.1.1.0 /24	s1
10.1.0.0 /16	s0
10.1.0.0 /24	e1
10.1.1.1 /32	s2

一个目标地址是10.0.4.1的分组到达该路由器，该路由器将使用哪个接口转发该分组？

解答：e1。最长匹配路由是10.0.0.0/16，它的输出接口是e1。

15．在主机仅有1个接口的情况下为什么主机还要有路由表呢？

解答：为了发送分组，主机仍然需要有路由表。这不仅因为需要路由表告诉主机缺省网关是哪个设备，而且还要定义网络的广播地址以及回送（loopback）接口。

如图6-6所示，像是PC和服务器这样的主机典型地是连接到多路访问的广播网络上。在这里可能有数百台甚至数千台设备连在同一个IP子网上，主机也可能有多个网关。

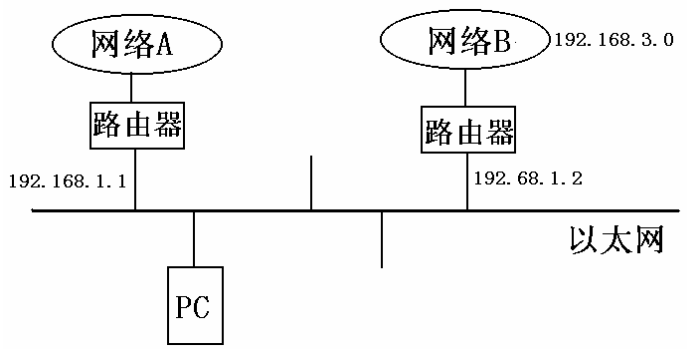


图 6-6　具有多个网关的主机

在我们给出的示例中，两台路由器跟一组PC连在同一网络上。如果PC的缺省网关是192.168.1.1，那么在它的路由表中将有下面列出的一条路由：

目标网络	网络掩码	网关	接口	度量
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.3	1

这就把其目的地不是指向本地网络的所有交通都送往192.168.1.1。显然这可能不是优化的路由选择，因为前往网络B的交通先要被送到路由器192.168.1.1，然后该路由器再把交通转发到192.168.1.2，最后，路由器192.168.1.2把交通转发到网络B。

为了解决这个问题，有两种方法可供选择。第一种是启用ICMP重定向。当路由器192.168.1.1接收到一个目的地址在网络B的分组时，它意识到这不是最佳的路由，因此它给PC发送一个ICMP重定向分组，告诉它经过192.168.1.2是最好的路由。然而，由于安全性的考虑，ICMP重定向常常被禁止。

第二种方法是手工配置如下一条路由：

目标网络	网络掩码	网关	接口	度量
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.3	1

192.168.3.0　　255.255.255.0 192.168.1.2　　192.168.1.3　　1

这样就可以让主机将分组直接送往连接网络B的路由器192.168.1.2　　。在这种情况下，192.168.1.2路由器是一个网关，但不是缺省网关。

16．水平分裂是怎样工作的？

解答：水平分裂禁止一个路由器在同一接口上通告一个在该接口上收到其路由信息的网络。在图6-7中，所有的路由器都使用RIP，在某个时间t=0路由器A向路由器C通告网络1具有1个跳段的代价。同时，路由器B向路由器D通告网络1。在路由器C的下一个更新期间，它向路由器E通告它的整个路由表，包括具有两个跳段代价的网络1。它还把在它的路由表中的这些路由通告给路由器A。在不实施水平分裂的情况下，这些路由中包括具有两个跳段代价的网络1。

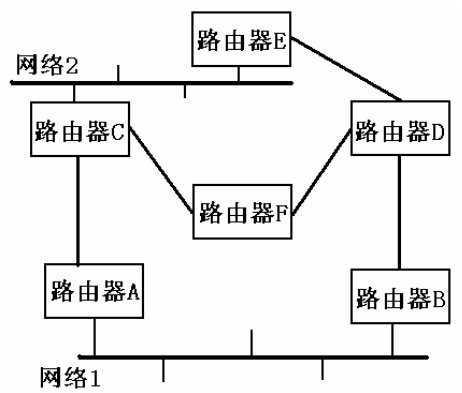


图 6-7　水平分裂

由于距离向量协议不保持关于通告的来源的信息，现在路由器A相信，它有两条路由可到达网络1：它自己直接连接的以太网接口，以及距离路由器C两跳段的路由。然而，由于它自己的接口是0跳段代价，所以它丢弃了后一条路由。

不久，路由器D向路由器E通告经过两个跳段可到达网络1，路由器E向路由器C通告经过3个跳段可到达网络1。路由器C丢弃这一信息，因为经过路由器A的通路要短得多。

到目前为止，一切都运行良好。但当A 的以太网接口出故障后情况就不同了。路由器A发送一个关于网络1具有16或无穷大代价的通告，表示通过路由器A不能够到达网络1。不幸的是，路由器A在可以发布这样的通告以前已经从路由器C收到了一个更新，说明路由器C经过两个跳段可以到达网络1。当然，路由器C和A都不知道这条路径实际上是通过一个现在已经不可用的接口。

在这一点上，如果网络2上的一个主机给网络1上的一个主机发送一个分组，路由器C把这个分组转发给路由器A。路由器A检查该分组，并把它转发给路由器C。路由器C检查它，把它又转发给路由器A。这一过程一直继续下去，直到分组的生命期超时。

水平分裂通过禁止把在一个接口上接收到的关于一个网络的路由信息再在同一接口上通告来阻止上述现象的发生。

17．　如图6-8所示，在配置了水平分裂的RIP网络聚合之后，路由器A的以太网接口失

效，那么网络对于这样的拓扑改变将会做出什么样的反应？

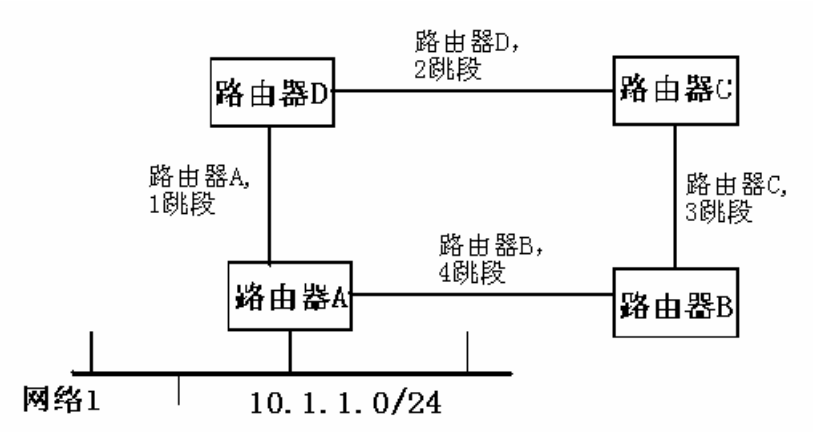


图 6-8　具有水平分裂的 RIP 网络

解答：当路由器A意识到它的以太网接口失效时，它开始寻找一个替代路由。因为路由器A和D正在使用水平分裂，路由器D不把网络10.1.1.0往回通告给路由器A，因此不会形成回路。

当到达网络10.1.1.0的路由通过网络传递时，它最终会到达路由器B，路由器B又把它传递回路由器A，其代价是4个跳段。路由器A接受该路由，并在下一个更新期把它广播到路由器D，其代价是5个跳段。

在这一点上，如果要把一个分组发送给10.1.1.100，路由器A将把它转发到路由器B，路由器B把它转发到路由器C，路由器C把它转发到路由器D，路由器D把它转发到路由器A。路由器A再次把它转发到路由器B，结果还是有回路。这个分组继续循环传送，直到生存时间值达到0为止。

为了防止这种类型的回路发生，距离向量协议使用一种计数到无穷大的技术。在这种情况下，无穷大被定义成16跳段，这也正是RIP为什么限于16跳段的原因。此时，路由器D从A接收到10.1.1.0 5个跳段的路由，把它以6个跳段计数往路由器C传递，路由器C把它以7跳段代价值传给路由器B。B再把它以8跳段代价值传给A。这一过程继续下去，直到最后路由器B向A广播一条16跳段代价的路由。

使用这个方法的问题是，路由聚合可能要花几分钟的时间。

18．为什么不使用“全0”和“全1”的子网？

解答：起初有4种类型的广播：

- 有限广播　　• 定向广播　　• 所有子网定向广播　　• 子网定向广播

有限广播是熟悉的255.255.255.255形式。之所以称为有限广播是因为不允许路由器转发它们。

定向广播和子网定向广播起初的用意是不同的，但现在已不加区别了。它们都是主机部分置成全1的网络地址。前者的例子有10.255.255.255；后者的例子有在划分子网

（10.1.0.0/16）情况下的10.1.255.255。

所有子网定向广播是把分组广播到一个特别的分类网络的所有子网，例如你的网络10.0.0.0有8位子网掩码，即10.1.0.0/16，其子网广播地址是10.1.255.255。广播到10.255.255.255的分组将被送到所有下列子网：

10.1.0.0
10.2.0.0
10.3.0.0
……
10.254.0.0

不幸的是，在路由表中不提交子网掩码的分类路由协议无法懂得10.0.0.0/16和10.0.0.0/8之间的差别。如果你要使用全1子网（10.255.0.0/16）并且发送到10.255.255.255，路由器将无法知道是所有子网，还是一个到10.255.0.0/16网络的一个定向广播。

因此，首先定义子网的RFC 950文档简单地禁止使用全1和全0子网。

今天都不使用所有子网的定向广播，无类别路由协议可以容易地懂得10.0.0.0/16和10.0.0.0/8之间的差别。因此在技术上没有理由不使用全0或全1子网。然而许多人倾向于不使用它们，因为它们可能引起混淆。

19．使用图6-9中所示的网络作为示例，说明定向广播是如何工作的？

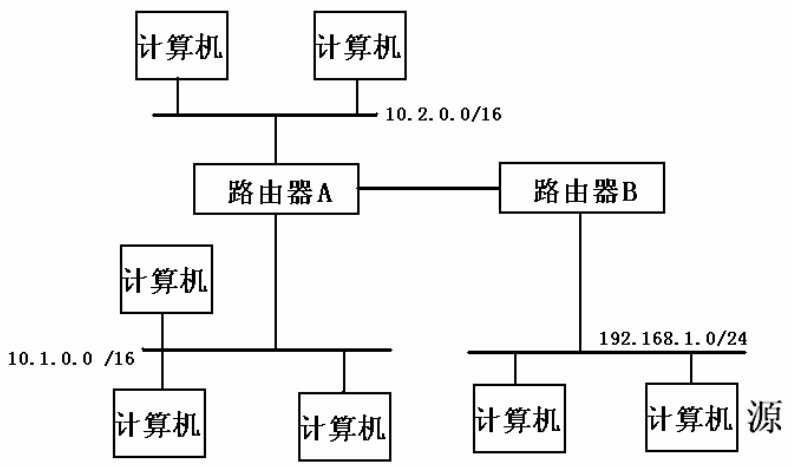


图 6-9　定向广播

解答：在图6-9中，如果标记成源的计算机要发送一个255.255.255.255的有限广播，它将仅被在它的本地网段上的计算机和路由器B接收和处理。

如果这个计算机又要发送一个定向广播到10.1.255.255，分组将被单播传送到路由器B，路由器B把分组转发给路由器A，路由器A把分组在包含10.1.0.0/16的以太网接口上传送，在这里它将被看成是一个广播，并且随后在那个子网上被所有的主机接收和处理。

如果同样的计算机要发送一个所有子网的定向广播到10.255.255.255，路由器B将把分组转发到路由器A，路由器A把分组既在包含10.1.0.0的网段的接口上，也在包含10.2.0.0的

网段的接口上发送。这就意味着在这些网段上的所有主机都会接收和处理这个分组。

幸运的是，今天人们已不再使用所有子网的定向广播。无类别路由协议可以区分10.0.0.0/16和10.0.0.0/8之间的差别。

20．给出如图6-10所示的支持组播的网络的共享树，其中R6是会聚点，对于一个连接到路由器R8的客户，要发送组播交通给连接到R1的一个客户，将会取哪一条通路？

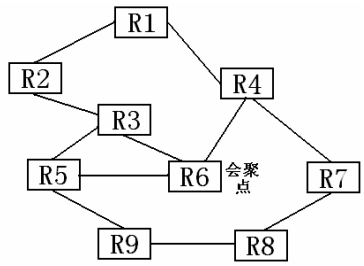


图 6-10　使用共享树的组播网络

解答：首先，R8把交通发送到会聚点（参见图6-11）。所经过的通路是R8-R9-R5-R6。当然，也可以取通路R8-R7-R4-R6。前者的通路是任意选取的。

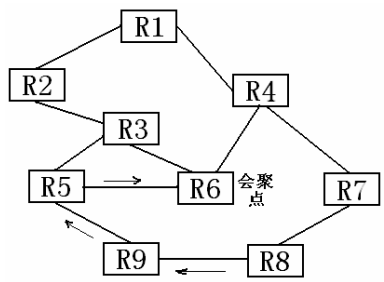


图 6-11　由 R8 送往会聚点的交通

组播分组一旦被会聚点接收，它就通过在其树中的最短通路（R6-R4-R1）转发。图6-12示出了树和通路。

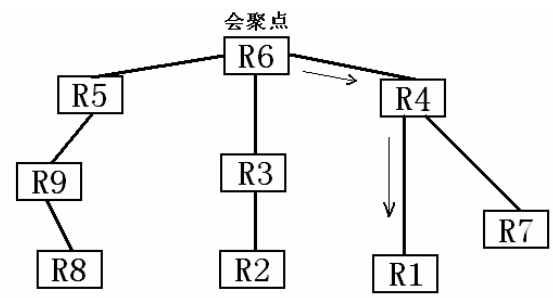


图 6-12　会聚点通过树中的最短通路转发交通

21．如果在图6-13中的网络是一个采用源树的网络，对于一个连接到路由器R8的客户，要发送组播交通给连接到R1的一个客户，又会取什么样的通路呢？

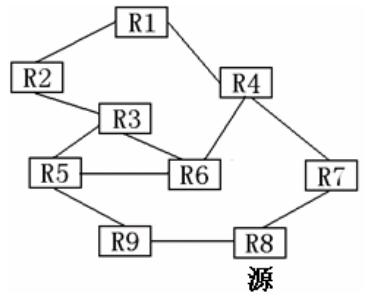


图 6-13　使用源树的组播网络

解答：先计算从R8到R1的最短通路树，示于图6-14。因此通路是R8-R7-R4-R1，因为源树总是从发送方的观点出发来建立，根总是发送方。

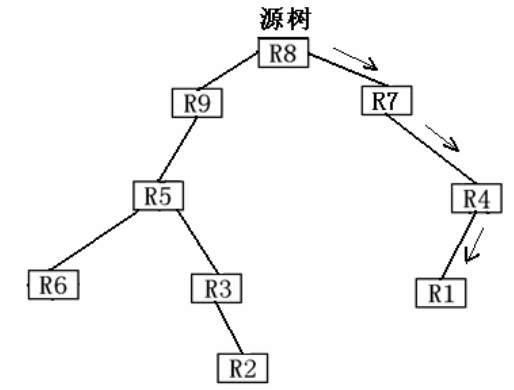


图 6-14　从 R8 到 R1 的最短通路树

22．使用图6-15所示的网络，从R6到R2，RIP协议倾向于选取哪一条通路？

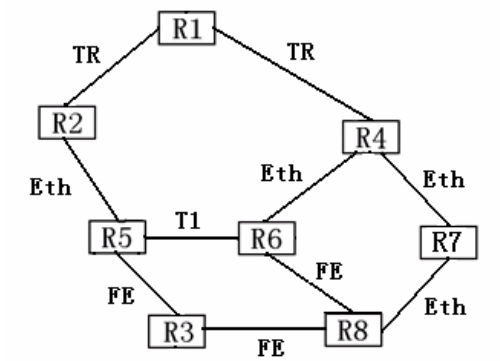


图 6-15　网段和链路

解答：R2使用1跳段计数把它的网络通告给R5和R1。R5把R2的网络以2个跳段计数通告给R6。R1把R2的网络以2个跳段计数通告给R4，R4把R2的网络以3个跳段计数通告给R6。因此，R6将取通过R5的具有2个跳段的最短通路，即R6-R5-R2。

23．如果在上题的图6-15中示出的网络使用OSPF代替RIP，那么从R6到R2倾向于选取哪一条通路？

解答：在这里，我们必须计算每条链路的代价。OSPF的缺省做法如下：

代价=参考带宽/接口带宽；
参考带宽的缺省值是100Mbps。
对于相关技术的接口带宽值如下：
T1=1.544Mbps,　以太网=10Mbs,　令牌环=16Mbps,　快速以太网=100Mbps。

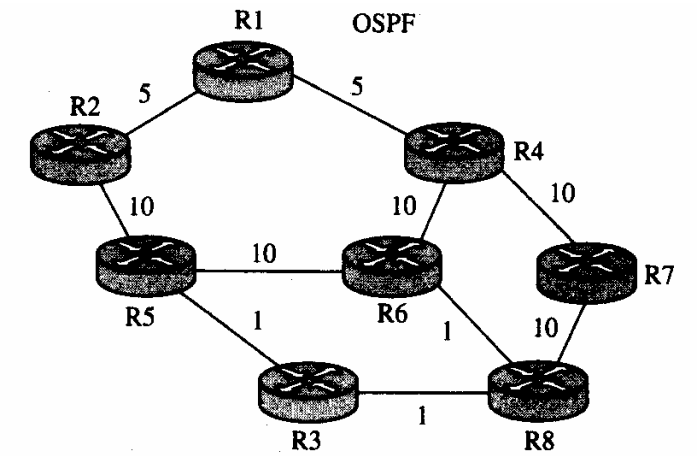


图 6-16　使用 OSPF 的网络链路代价

因此，如图6-16所示，
T1链路的代价是100/1.544=65
以太网段的代价是100/10=10
令牌环网段的代价是100/16=6
快速以太网段的代价是100/100=1。

要计算一条通路的代价，只须把通路上的各条链路的代价加在一起，

R6,R5,R2 = 75
R6,R4,R1,R2 = 22
R6,R8,R3,R5,R2 = 13
R6,R8,R7,R4,R1,R2 = 33
显然，最后选取得是高速通路R6-R8-R3-R5-R2。

24．如图6-17所示，在用手工改变上题中的链路代价后，在R6和R2之间将倾向于选取哪一条通路？

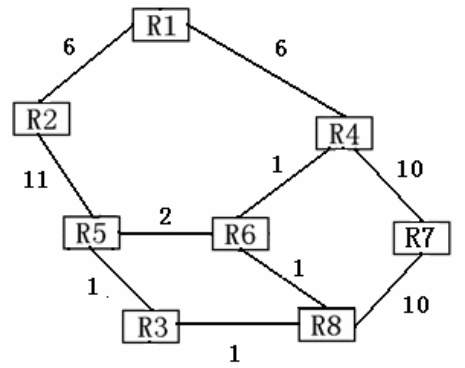


图 6-17　修改后的链路代价

解答：计算各条通路的代价，得到：

R6,R5,R2 = 13
R6,R4,R1,R2 = 13
R6,R8,R3,R5,R2 = 14
R6,R8,R7,R4,R1,R2 = 33
此时有两条相同代价的通路，同时选取这两条通路，即：
R6-R5-R2 和R6-R4-R1-R2 。
OSPF可以支持多达4条相同代价通路的负载平衡。

25．大多数IP路由选择协议都使用跳段数作为在做路由计算时设法使其取值最小的一种度量。而对于ATM网络而言，跳段数不是很重要。为什么？ATM网络也使用存储-转发机制吗？

解答：IP使用存储-转发的分组交换机制。分组在被完全存储后，才能进行转发。存储一个分组以及然后再发送的时间通常都超过在线路上的传输时间。因此，存储-转发网络试图通过减少跳段数来避免这一操作。ATM交换机使用虫孔路由选择，即在得到5个字节的头之后，它们就开始发送。因此，在每个交换机中仅有很少的延迟。在这种情况下，减少所跨越的交换机的数目就显得不是那么关键。

26．在IP和ATM中，检验和都是仅覆盖头部而不包括数据。试说明这样设计的理由。

解答：在头中的错误比在数据中的错误更严重。例如，一个坏的地址可能导致分组被投递到错误的主机。许多主机并不检查投递给它们的分组是否确实是要投递给它们的。它们假定网络从来不会把本来是要前往另一主机的分组投递给它们。有的时候数据不参与检验和的计算，因为这样做代价大，上层协议通常也做这种检验工作，从而引起重复和多余。

27．一个居住在华盛顿的人带着他的便携式计算机到波士顿旅行。使他没有料到的是，在波士顿的目的地的LAN是一个无线IP LAN。那么，为了使得电子邮件以及其它交通能正确地到达原居所，他仍然必须通过本地代理和外部代理这样的一整套过程吗？

解答：在回答这一问题之前，我们需要搞清楚移动IP的概念。允许其用户漫游的每个

场点都必须建立一个本地代理。允许外界访问的每个场点都要建立一个外部代理。当一个移动主机抵达一个外部场点时，它跟那里的外部代理主机联系，并进行登记。然后，该外部代理主机跟移动用户的原居住地的本地代理联系，并给它一个转交地址，通常就是该外部代理的IP地址。

当一个分组到达用户的本地LAN时，它进入连接到该LAN的某个路由器。路由器然后尝试以通常的方式寻找主机的位置。它广播一个ARP分组，询问（例如）“160.80.40.20”的以太网地址是什么？“ 本地代理通过给出自己的以太网地址来应答这个询问。路由器把前往160.80.40.20的分组发送给本地代理。本地代理又以隧道通信的方式把分组发送给转交地址，即前往外部代理。外部代理再取出IP分组，并投递到移动主机的数据链路地址。此外，原居住地的本地代理把转交地址提供给发送方，使得随后的分组可直接地隧道发往外部代理。

现在我们回到本习题的解答。答案是仍然需要通过上述的本地代理和外部代理的一整套过程。实际上，波士顿的局域网是无线网的事实并不会使得到达华盛顿发给该用户的分组会突然地跳到波士顿。在华盛顿市的本地代理必须把分组以隧道方式传给在波士顿的无线LAN上的外部代理。看待这一问题的最好方法是用户必须接入波士顿的LAN，并且是以跟在波士顿的其它用户一样的方式接入。连接是使用无线还是有线不是关键问题。

28．IPv6使用16字节地址。如果每微微妙分配一个含有100万个地址的地址块，那么该16字节地址可持续多长时间？

解答：使用16个字节，总的地址数为2^{128}或3.4×10^{38}。如果我们以没微微秒10^{6}，亦即每秒10^{18}的速率分配它们，这些地址将持续3.4×10^{20}秒，即大约10^{13}年的时间。这个数字是宇宙年龄的1000倍。当然，地址空间不是扁平的，因此它们的分配非线性，但这个计算结果表明，即使分配方案的效率为千分之一，这么多地址也永远都不会用完。

29．在IPv4的头中使用的协议段在IPv6的固定头中不复存在。试说明这是为什么？

解答：设置协议段的目的是要告诉目的地主机把IP分组交给哪一个协议处理程序。中途的路由器并不需要这一信息，因此不必把它放在主头中。实际上，这个信息存在于头中，但被伪装了。最后一个（扩展）头的下一个头段就用于这一目的。

30．当采用IPv6协议的时候，ARP协议是否需要改变？如果需要，是概念上的改变，还是技术上的改变？

解答：从概念上讲，不需要改变。在技术上，由于被请求的IP地址现在变大了，因此需要比较大的域（也称段）。

31. 一个单位有一个C类网络200.1.1。考虑到共有四个部门，准备划分子网。这四个部门内的主机数目分别是：A—72台， B—35台， C—20台， D—18台； 即共有145台主机。

（a）给出一种可能的子网掩码安排来完成划分任务

解答：每个部门分配一个子网，名义上部门A、B、C、D的子网大小分别是：

2^7（=128），2^6（=64），2^5（=32）和2^5（=32）

IP地址的最高位是0表示子网A，最高两位是10表示子网B，最高三位是110表示子网C，最高三位是111表示子网D。显然这里采用了可变长子网掩码，涉及3种子网掩码，分别是

255.255.255.128

255.255.255.192

255.255.255.224

（b）如果部门D的主机数目增长到34台，那么该单位又该怎么做？

解答：给部门A分配两个子网01和001，名义上分别是64个地址和32个地址，共96个地址；

部门B不变，仍然是10，名义上大小为64个地址；

部门C改为000，名义上大小是32个地址

部门D改为11，名义上大小是64个地址。

32. 让ARP登录项在10-15分钟后超时是进行合理的折中的一种尝试。试说明如果把超时值定得太小或太大可能引发的问题。

解答：如果超时值太小，我们将给网络加载不必要的重复请求，直到收到对请求的应答才停止发送。

当一台主机的以太网地址改变时，例如由于网卡的更换，那么对于那些在其ARP缓存中仍维持该主机的旧的以太网地址的结点来说，该主机是不可达的。这显然是把超时值定得太大可能引发的问题。

10-15分钟似乎是关闭主机、交换以太网卡和重引导所需要的最少时间量。对于太长超时值问题的一种可能的解决办法是自我ARP，启动时在网上对自己的IP地址做ARP查询广播，同时让其他主机在看到来自在缓存中已有登录项的主机的ARP请求时更新它们的缓存。然而这类措施并未普遍实行，所以需要有一个合理的ARP缓存超时的上限值作为备份途径。

33. 在使用ARP的同一个以太网上，假定主机A和B被分配同一个IP地址，并且B在A之后启动。那么，这对于A的现有连接会有什么影响？试给出克服这一影响的一种措施。

解答：在B广播任何ARP询问之后，先前给A的物理地址发送的所有站都转为给B的物理地址发送。A将看到所有到达的交通突然停止。为预防此类事件，A可以有意地监视跟自己的IP地址有关的ARP广播，A甚至可以紧随这样的广播做自己的ARP广播，以使流往自己的交通得以恢复。

如果B在启动时使用自我ARP，它将收到一个应答，表明它的IP地址已被使用，这就意味着B在地址冲突问题解决之前不应该继续在网络上驻留。

34. 假定主机A和B在一个具有C类IP网络地址200.0.0的以太局域网上。现在通过一条对B的直接连接把主机C附接到该网络（参见图6-18）。说明对于这种配制如何划分子网，并给出一种具体的样例子网地址分配。假定不可能提供额外的网络地址。这对以太局域网的大小会有什么影响？

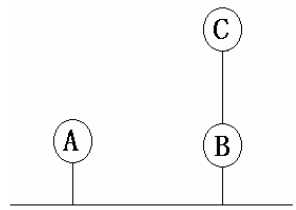


图 6-18　习题 34 插图

解答：考虑到路由选择，C必须有自己的子网。尽管这个子网很小，但它也减少了原先的以太网可提供的主机数，现在主机号最多只能是7位二进制。下面的表6-1给出的是主机B的一种可能的路由选择表，其中子网号和掩码的最后一个字节都用二进制表示。注意，有些地址不匹配这两个子网中的任何一个。

表6-1　主机B的一种可能的路由选择表

网络	子网	掩码	接口
200.0.0	0/0000000	1000 0000	以太网
200.0.0	100000/00	1111 1100	直接链路

35. 表6-2是使用无类别域间路由选择（CIDR）的路由选择表，地址字节是用十六进制表示的。在C4.50.0.0/12中的“/12”表示开头有12个1的网络掩码，也就是FF.F0.0.0。注意，最后三个登录项涵盖每一个地址，因此起到了缺省路由的作用。试指出具有下列目标地址的IP分组将被投递到哪一个下站地？

表6-2　路由选择表

网络/掩码长度	下一站地
C4.50.0.0/12	A
C4.5E.10.0/20	B
C4.60.0.0/12	C
C4.68.0.0/14	D
80.0.0.0/1	E
40.0.0.0/2	F
00.0.0.0/2	G

（a）C4.5E.13.87

解答：网络号C4.5E.10.0/20（下一站地是B）的第3字节可以用二进制表示成0001 0000。

目标地址C4.5E.13.87的第3字节可以用二进制表示成0001 0011，显然取20位掩码与网络号C4.5E.10.0/20相匹配，所以具有该目标地址的IP分组将被投递到下站地B。

（b）C4.5E.22.09

解答：网络号C4.50.0.0/12（下一站地是A）的第2字节可以用二进制表示成0101 0000。

目标地址C4.5E.22.09的第2字节可以用二进制表示成0101 1110，显然取12位掩码与网络号C4.50.0.0/12相匹配，所以具有该目标地址的IP分组将被投递到下站地A。

（c）C3.41.80.02

解答：网络号80.0.0.0/1（下一站地是E）的第1字节可以用二进制表示成1000 0000。

目标地址C3.41.80.02的第1字节可以用二进制表示成1100 0011，显然取1位掩码与网络号80.0.0.0/1相匹配，所以具有该目标地址的IP分组将被投递到下站地E。

（d）5E.43.91.12

解答：网络号40.0.0.0/2（下一站地是F）的第1字节可以用二进制表示成0100 0000。

目标地址5E.43.91.12的第1字节可以用二进制表示成0101 1110，显然取2位掩码与网络号40.0.0.0/2相匹配，所以具有该目标地址的IP分组将被投递到下站地F。

（e）C4.6D.31.2E

解答：网络号C4.60.0.0/12（下一站地是C）的第2字节可以用二进制表示成0110 0000。

目标地址C4.6D.31.2E的第2字节可以用二进制表示成0110 1101，显然取12位掩码与网络号C4.60.0.0/12相匹配，所以具有该目标地址的IP分组将被投递到下站地C。

（f）C4.6B.31.2E

解答：网络号C4.68.0.0/14（下一站地是D）的第2字节可以用二进制表示成0110 1000。

目标地址C4.6B.31.2E的第2字节可以用二进制表示成0110 1011，显然取14位掩码与网络号C4.68.0.0/14相匹配，所以具有该目标地址的IP分组将被投递到下站地D。

36. 在图6-19中的网络使用RSVP，主机1和2的组播树如图所示。假定主机3请求一个带宽为2MB/秒的通道用于来自主机1的流，请求另一个带宽为1 MB/秒的通道用于来自主机2的流。同时，主机4请求一个带宽为2MB/秒的通道用于来自主机1的流，主机5请求一个带宽为1MB/秒的通道用于来自主机2的流。那么，在路由器A、B、C、E、H、J、K和L上要为这些请求预留多大的总带宽？

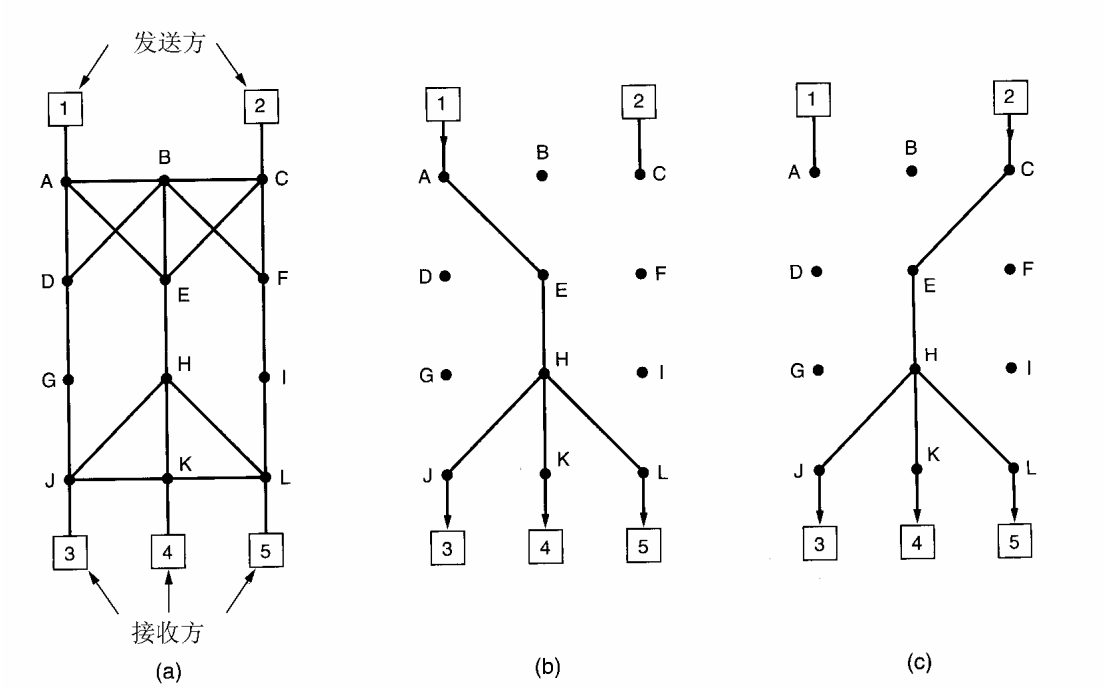


图 6-19 (a)一个网络　(b)主机 1 的组播分布树 (c) 主机 2 的组播分布树

解答：以MB/秒为单位表示带宽

A：2，　B：0，　C：1，　E：3，　H：3，　K：2，　L：1

37. 考虑带有加快转发机制的差分服务的用户。有保证服务的加快分组一定经历比常规分组较短的延迟吗？请说明你的答案的理由。

解答：没有保证。如果有太多的分组被加快，它们的通道可能具有比常规通道甚至更坏的性能。

38. 假定主机A连接到路由器R1，R1连接到另一个路由器R2，R2连接到主机B。假定一个含有900字节数据和20字节TCP头的TCP报文传递到主机A的IP代码，目的地是

主机B。示出在这三条链路上发送的每个分组中IP头的中长度域、标识符域、不许分割域、还有片段域和分片偏移域的值。假定链路A-R1可以支持的最大帧长是1024字节，其中包括14字节的帧头；链路R1-R2可以支持的最大帧长是512字节，其中包括8字节的帧头；R2-B可以支持的最大帧长是512字节，其中包括12字节的帧头。

解答：初始的IP数据报载R1被分割成两个IP数据报，沿途中不会再发生其它的分割。

链路A-R1:

总长度=940字节；标识符=x；不许分割=0；还有片段=0；偏移=0

链路R1-R2:

（1）总长度=500字节；标识符=x；不许分割=0；还有片段=1；偏移=0

（2）总长度=460字节；标识符=x；不许分割=0；还有片段=0；偏移=60单位（单位是8个字节）

链路R2-B:

（1）总长度=500字节；标识符=x；不许分割=0；还有片段=1；偏移=0

（2）总长度=460字节；标识符=x；不许分割=0；还有片段=0；偏移=60单位（单位是8个字节）

39. 考虑在图6-20中的示例互联网，其中源D和E给组G发送分组，组G的成员在图中用带阴影的方块表示。试为每个源画出最短通路组播树。

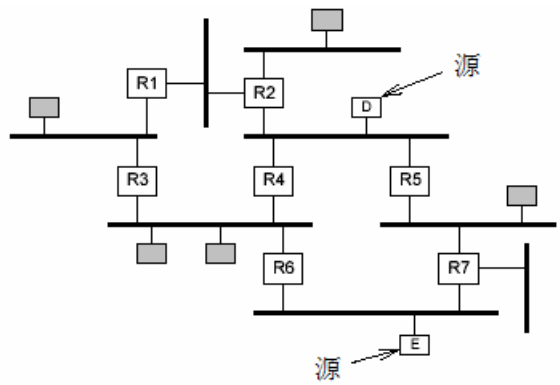


图 6-20　习题 39 插图

解答：见图6-21。

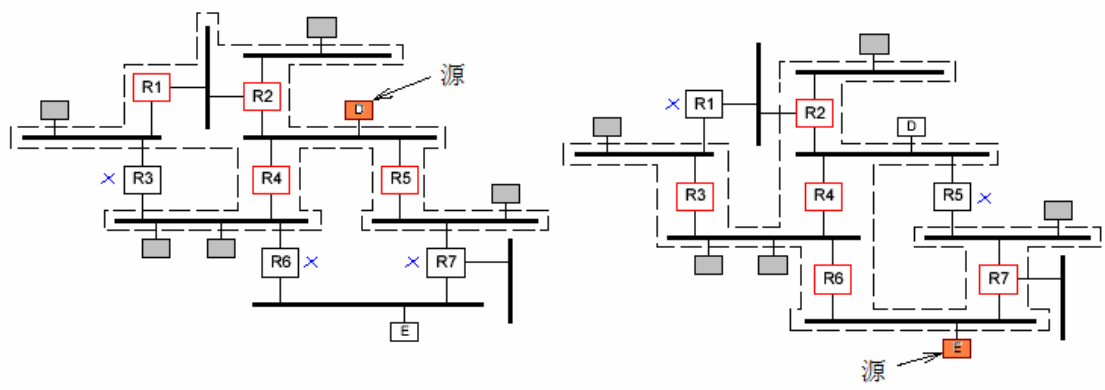


图 6-21　为每个源画的最短通路组播树

40. 假定主机A给一个组播组发送，接收方是以A为根深度为N的一棵树，其中每个非叶节点都有k个孩子；因此共有k^N个孩子。

（a）如果A发送一个组播报文给所有的接收方，那么要涉及多少次链路传输？

解答：除了一个根节点外，各个深度的节点数如下：

深度　　节点数　　节点类型

1	k	非叶节点
2	k^2	非叶节点
3	k^3	非叶节点
…	…	…
N-1	k^{N-1}	非叶节点
N	k^N	叶节点

组播的任务是将组播分组传输到叶节点所在的物理网络上的指定路由器，从指定路由器到每个叶节点的链路传输次数依赖网络的拓扑，计算时可以不予考虑，因为不排除有组播分组到达本地广播网上的指定路由器也就可以被目标叶节点接收到的可能性。所以在本小题中组播涉及的链路传输总次数为：$k+k^2+k^3+ \ldots +k^{N-1}+ k^N = (k^N-k) / (k-1)$

（b）如果A发送单投点报文到每个接收者，那么要涉及到多少次链路传输？

解答：在单投点传输中，目的地网络的路由器每一次只能针对一个目的地接收者发送分组，并且至少涉及1次链路传输，即使有多个目的地接收者在同一个广播网络上也如此。在本小题中，1次单投点传送涉及N条链路，所以发送到每一个接收方总的链路传输次数为：$N \times k^N$

（c）假定A给所有的接收方发送，但一些报文丢失了，需要重传。就使用链路的次数而言，对多大比例的接收方做单投点重传等同于对所有接收方的组播重传？

解答：对x比例的接收方做单投点传输涉及的链路传输次数为：$x \times N \times k^N$

我们已经知道，A发送一个组播报文给所有的接收方所涉及的链路传输次数是$(k^N-k) / (k-1)$

从方程 $x \times N \times k^N = (k^N-k) / (k-1)$

得到：$x =[(k^N-k) / (k-1)] / [N \times k^N] \approx 1 / [(k-1) \times N]$

41.一个路由器爆发出大量其长度为1024字节（数据+头部）的IP分组。假定分组的存活期为10秒，那么要免除IP数据报的标识符号码循环回来重复的危险，路由器可以运行的最大线路速度是多大？

解答：1024×8=8192

如果线路的位速率是b，路由器可以发送的每秒分组数是b/8192，因此它发送一个分组所花的秒数是8192/b。发送65536个分组花的秒数是$2^{16} \times 2^{13}/b=2^{19}/b$。让这个时间跟最大分组存活期相等，我们得到

$2^{29}/b=10$，因此b的值大约为53,687,091 bps。

42. 一个使用严格源路由选择选项的IP数据报必须被分割。你认为是把选项域拷贝到每个片段，还是仅把它放进第一个片段就可以了？请解释你的答案。

解答：因为路由每一个片段都需要该信息，所以选项必须出现在每一个片段中。

43. 从198.16.0.0起有大量相继的IP地址可提供。假定4个单位A、B、C和D分别请求4000、2000、4000和8000个地址，并且就按照所请求的顺序分配。对于这些单位中的每一

个，请给出分配的第一个IP地址、分配的最后一个IP地址，以及用w.x.y.z/s形式表示的掩码。

解答：作为开始，把这些请求向上提升成2的幂，那么

	开始地址	结束地址	掩码
A	198.16.0.0	198.16.15.255	198.16.0.0/20
B	198.16.16.0	198.23.15.255	198.16.16.0/21
C	198.16.32.0	198.47.15.255	198.16.32.0/20
D	198.16.64.0	198.95.15.255	198.16.64.0/19

44.一个路由器刚收到下列新的IP地址：

57.6.96.0/21
57.6.104.0/21
57.6.112.0/21
57.6.120.0/21

如果它们都使用同样的输出线路，它们可以被聚合吗？如果可以，怎样聚合？如果不可以，为什么？

解答：它们的地址的前两个字节相同，第三个字节的前三位都是011，它们可以聚合成57.6.96/19。

45. 一组从29.18.0.0到19.18.128.255的IP地址被聚合成29.18.0.0/17。然而，有从29.18.60.0到19.18.63.255的1024个未被分配的地址间隙，现在突然被分配给使用一个不同的输出线路的主机。现在还需要把聚合地址分裂成多于一个的连续的地址快，并把新的块加入路由表，那么是否可以重新聚合？如果可以，怎样聚合？如果不可以，又怎样做？

解答：只要为新的地址块增加一个新的表项29.18.0.0/22就可以了。如果有一个入进分组同时匹配29.18.0.0/17和29.18.0.0/22,选取最长匹配。这一规则使得有可能把一个大的地址块分配给一个外出线路，而让一个或多个在此范围内的小的地址块作为例外来处理。

46.一个路由器在它的路由表中有下列无类别域间路由选择（CIDR）登录项：

地址/掩码	下一跳段
135.46.56.0/22	接口0
135.46.60.0/22	接口1
192.53.40.0/23	路由器1
缺省	路由器2

对于下列每一个IP地址，如果具有那个地址的一个分组到达，路由器怎么处理？

（a）135.46.63.10 **解答**：外出接口选择接口1
（b）135.46.57.14 **解答**：外出接口选择接口0
（c）135.46.52.2 **解答**：外出接口选择路由器2
（d）192.53.40.7 **解答**：外出接口选择路由器1

（e）192.53.56.7　　**解答：**外出接口选择路由器2

47. 许多公司的策略都是用两个（或更多个）路由器把公司连接到Internet，以提供一些冗余，防止它们失效时失去连接性。在这种策略下，还可能使用NAT吗？

解答：在安装NAT之后，关键的一点是属于单条连接的所有分组要通过同一台路由器进入和离开公司。如果每个路由器都有它自己的IP地址，并且属于一条给定连接的所有交通可以被送往同一个路由器，映射可以正确进行，NAT的多宿主机也可以正常工作。

第 7 章　运 输 层

本章学习重点

- 运输层服务
- 运输层寻址
- TCP报文段
- UDP数据报
- TCP连接的建立和释放
- 运输层协议的发展

7.1　基本知识点

运输层是整个协议体系得中心，它的任务是提供可靠的、代价有效的从源到目的地机器的数据传输，并且独立于物理网络或当前使用的网络。没有运输层，层次协议的概念将会变得没有意义。

运输层通常是向应用层中的进程提供服务。它使用由网络层提供的服务。执行运输层功能的软件或硬件称作运输实体。运输层实体可以放在操作系统内核中，也可以放在一个单独的用户进程中，在捆绑到网络应用的库程序包中，或者在网络接口卡上。

运输服务由在两个运输实体之间的运输协议实现。就完成的功能而言，运输协议在某些方面类似于数据链路层协议，它们都必须做差错控制、排序和流控制。

然而，在这两种协议之间也存在着显著的差别。在数据链路层，两个设备通过物理通道直接通信；而在运输层，两台主机之间的运输连接可能通过多个子网。数据链路层通常不需要设备在一个端口上指定要跟哪个路由器通信，每条外出线路唯一地指定了一个特别的路由器；在运输层则需要明确的目的地寻址信息。数据链路层在导线上建立连接的过程是简单的，因为另一端总是存在；而在运输层，初始的连接是比较复杂的。

另外，在运输层有潜在的存储容量问题。如果网络内部使用数据报和自适应路由选择，分组有可能被存储几秒钟，然后再投递。

两种协议之间的最后一个差别是连接的数量。两个层次都需要缓冲和流控，但运输层连接数量大，且动态变化，需要有跟数据链路层不同的处理方法。在数据链路层，某些协议为每条线路分配固定数量的缓冲区，使得一个帧到达时总有一个缓冲区可提供。在运输层，必须管理的大量连接使得为每条连接专门分配许多缓冲区的思想不再具有吸引力。

就服务而言，运输层服务跟网络层服务更为相似。它们都提供面向连接的和无连接的两种类型的服务。两个层次的寻址和流控制也类似。然而，运输代码整个运行在用户机器

上，而网络层大部分运行在由承载商运营的路由器上。

运输层的存在使得传输服务有可能比基础网络服务更可靠。丢失了的和被破坏了的数据可以被运输层检测到和做补偿恢复。我们可以把运输服务原语实现为库过程，从而使得它们独立于网络服务原语。网络服务从一个网络到另一个网络可能变化很大，例如，无连接的LAN服务跟面向连接的WAN服务就有显著的差别。通过把网络服务隐藏在一组运输服务原语的后面，改变网络服务只需把一组库过程用另一组表示由新的基础网络完成的不同网络服务的库过程替换。

有了运输层，应用程序设计人员可以根据一组标准的原语编写程序，并且让这些程序在广泛种类的网络上工作，而不用担心处理不同的网络接口和不可靠的传输问题。把上层跟网络的技术、设计和不完善隔离开来是运输层完成的关键功能。

通常，人们把1到4层跟更高层次相区别。底部4层被看成是传输服务提供者，而更高的层次是传输服务用户。这种提供者跟用户的区别对协议层次的设计有相当大的影响，并把运输层放到了关键的位置，因为它形成了在可靠数据传输服务的提供者和用户之间的主要边界。

7.1.1 运输层服务

为说明运输服务的思想，考察表7-1中示出的5个最基本的服务原语。这种运输接口允许应用程序建立、使用和释放连接。它假定在服务器上有一个应用程序，并且有多个远程客户。

表7-1 简单的运输服务原语

原语	发送的分组	含义
LISTEN	(无)	阻塞，直到某个进程尝试连接
CONNECT	CONNECT REQ.	主动尝试建立连接
SEND	DATA	发送信息
RECEIVE	(无)	阻塞，直到有一个数据分组抵达
DISCONNECT	DISCONNECT REQ.	这一方要释放连接

开始，服务器执行LISTEN原语，典型地是调用一个库过程，该过程做系统调用，阻塞服务器，直到有一个客户到达为止。当有一个客户要跟服务器对话时，它执行CONNECT原语。运输实体执行这个原语，阻塞呼叫方，给服务器发送一个分组，封装在这个分组中的载荷是给服务器运输实体的运输层报文。

我们不妨把运输实体发送的报文称作TPDU(运输协议数据单元)。TPDU包含在网络层交换的分组中，分组包含在数据链路层交换的帧中。当有一个帧到达时，数据链路层处理帧头，并把帧的载荷段的内容向上传递给网络实体。网络实体处理分组头，并把分组载荷的内容向上传递给运输层。

再回到我们的客户-服务器的例子。客户的CONNECT调用引起一个CONNECT REQUEST TPDU发往服务器。当它到达时，运输实体检查后发现服务器被阻塞在LISTEN。运输实体解锁服务器，并给客户发回一个CONNECT ACCEPTED TPDU。当这个TPDU到达

时，客户被解锁，连接建成。

现在可以使用SEND和RECEIVE原语交换数据。在最简单的形式中，任一方 都可以做一个（阻塞）RECEIVE，等待另一方发送SEND。当该TPDU到达时，接收方被解锁，然后它可以处理该TPDU并发送一个应答。只要双方保持跟踪轮到谁发送，这一机制可以工作得很好。

每一数据分组最终都将被确认。载有控制TPDU的分组也被明确地或隐含地确认，这些确认由运输实体管理，使用网络层协议，并且对运输层的用户不可见。类似地。运输实体还处理超时和重传，所有这些机制都对运输用户遮蔽。

当连接不再被需要时，它必须被释放，以腾出在两个运输实体内的表空间。断连有两种方式：非对称和对称。在非对称的断连中，任一方运输用户都可以发出一个DISCONNECT原语，引起一个DISCONNECT REQ. TPDU发往远方运输实体。当它到达时，连接被释放。

在对称的断连中，连接在每个方向上分别关断，独立于另一方向。当一方做DISCONNECT时，意味着它没有更多的数据要发送，但仍然愿意从对方接收数据。在这个模型中，当双方都做了DISCONNECT后，连接才释放。

另一组实用的运输原语是在Berkeley UNIX 中用于TCP的套接口原语。这些原语广泛地用于Internet编程。表7-2示出了这些原语。

表7-2 用于TCP的套接口原语

原语	含义
SOCKET	建立一个新的通信端点
BIND	把一个本地地址附接到陶接口
LISTEN	宣告愿意接受连接，给出队列大小
ACCEPT	阻塞呼叫方，直到有一个连接尝试到达
CONNECT	主动尝试建立一条连接
SEND	在连接上发送数据
RECEIVE	在连接上接收数据
CLOSE	释放连接

开头4个原语由服务器依次执行。SOCKET原语建立一个新的端点，并在运输实体内为它分配表空间。调用的参数指定所使用的地址格式、需要的服务类型（例如可靠字节流）和协议。成功的SOCKET调用返回一个普通的文件描述符，用于随后的调用。OPEN调用做同样的工作。

新建的套接口没有网络地址。网络地址使用BIND原语分配。一旦服务器把一个地址绑定到套接口，远程用户就可以连接到它。不让SOCKET调用直接建立一个地址的原因是一些人比较介意他们使用的地址，因为他们可能已经使用一个地址许多年，每个人都知道这个地址；而另外一些人可能并不介意使用哪一个地址。

接下来是LISTEN调用，分配空间，排队进入的呼叫，主要考虑可能有好几个客户同时尝试连接。跟我们在前面给出的示例不同，在套接口模型中LISTEN是一个不阻塞的调用。

为了阻塞等待一个进入的连接，服务器执行一个ACCEPT原语。当有一个请求连接的

TPDU到达时，运输实体建立一个跟起初的套接口具有同样性质的新套接口，并为该连接返回一个文件描述符。然后服务器可以卵生一个进程或线程，用以处理在该新套接口上的连接，并转回到起初的套接口上等待下一个连接。ACCEPT返回一个通常使用的文件描述符，该描述符可被用以跟文件同样的标准方式读和写。

在客户那一边，首先使用SOCKET原语建立一个套接口，但不需要BIND，因为使用哪一个地址不为服务器所介意。CONNECT原语阻塞呼叫方，并主动地起动连接过程。当它完成时（即收到来自服务器的适当的TPDU）,客户进程解锁，连接建成。现在双方都可以使用SEND

和RECEIVE在全双工连接上发送和接收数据。如果不需要特别的SEND和RECEIVE选项，也可以使用标准的UNIX READ和WRITE系统调用。

套接口的连接释放是对称的，当双方都执行了CLOSE原语时，连接被释放。

7.1.2　运输层寻址

当一个应用进程要跟一个远地应用进程建立一条连接时，它必须指定要连接到谁。无连接运输也有同样的问题，即应该把报文送给谁。通常使用的方法是定义进程可以在其上倾听连接请求的运输地址。在Internet中，这些端点被称作端口。在ATM网络中，它们被称作AAL-SAP。我们在本书中使用通用的术语TSAP(运输服务访问点)。类似地，网络层地址称作NSAP（网络服务访问点）。IP地址就是NSAP的一个例子。

图7-1示出了一个可能的运输连接过程。

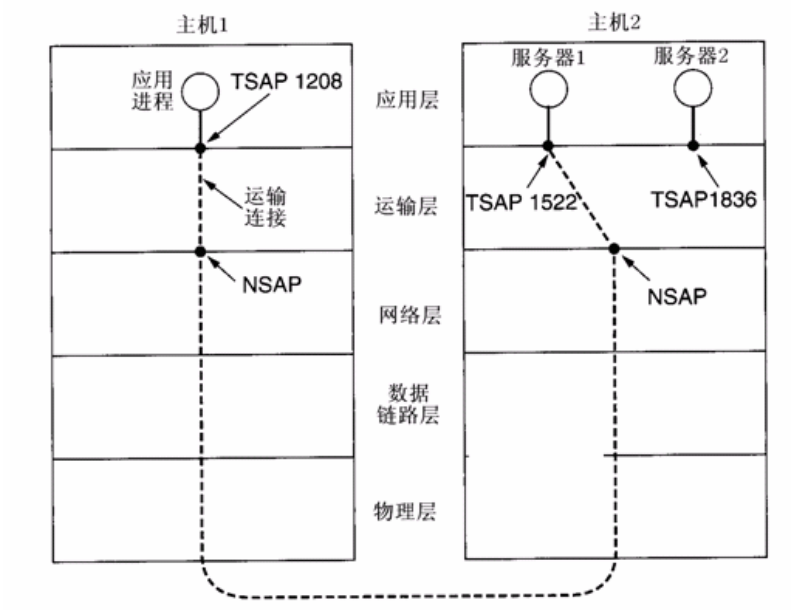


图 7-1　TSAPNSAP 和运输连接

（1）在主机2上的时间服务器把自己附接到TSAP 1522等待入进呼叫。作为例子，可以使用LISTEN。

（2）在主机1上的一个应用进程要查询时间，因此它发送一个CONNECT请求，指定TSAP 1208作为源，TSAP 1522作为目的地。这一动作的最终结果产生在主机1上的应用进程和主机2上的服务器1之间的一条运输连接。

（3）应用进程然后发送一个时间请求。

（4）时间服务器用当前的时间响应。

（5）然后运输连接被释放。

注意，在主机2上还可能有其它的服务器，附接到其它TSAP，等待在同一NSAP上到达的入进连接。

一些众所周知的服务具有稳定的TSAP地址，这些TSAP列在大家都知道的地方，例如UNIX系统上的/etc/services，说明哪些服务器永久地附接到什么样的端口。

然而，其它用户进程仅存在比较短的时间，没有事先广泛为人知道的TSAP地址，而且有许多服务器进程很少被使用，让它们每一个都处于活动状态，并一直在稳定的TSAP地址上倾听是浪费的。

一种解决方案如图7-2所示，它被称作初始连接协议。不是让每一个可能的服务器都各自在一个众所周知的TSAP上倾听，而是让愿意为远方用户提供服务的每个机器有一个特别的进程服务器，作为不常使用的服务器的代理。该代理同时倾听一组端口，等待连接请求。潜在的服务用户开始做一个CONNECT请求，指定他们想要的服务的TSAP地址。如果没有服务器在等待他们，他们就被连接到进程服务器，如图7-2（a）所示。

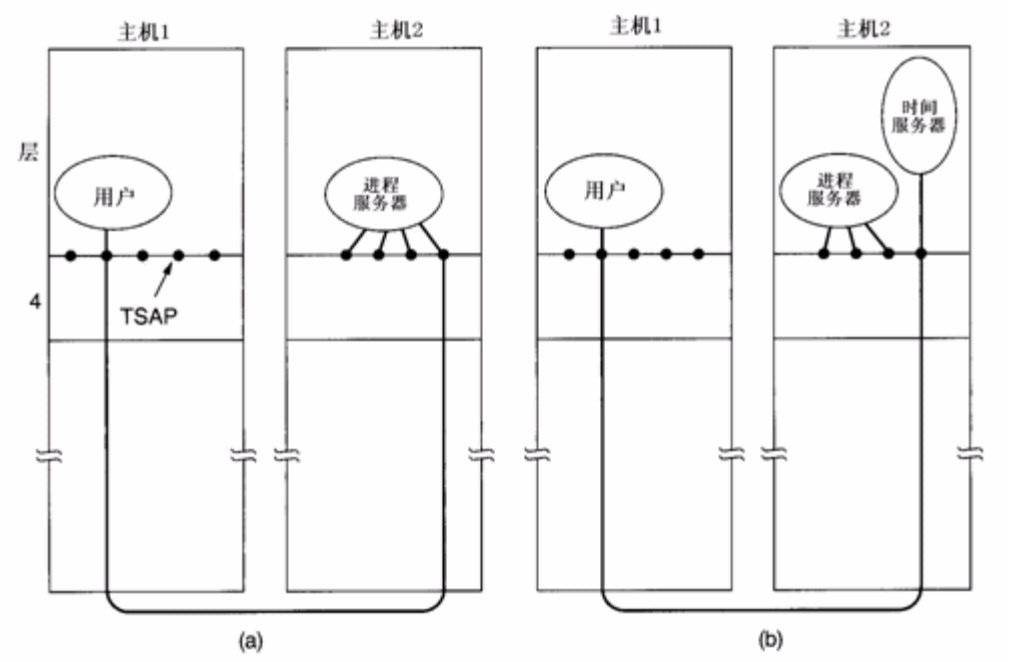


图 7-2　初始连接协议

在得到入进请求之后，进程服务器卵生所请求的服务器，允许该服务器继承跟用户的现有连接。然后，新的服务器执行请求的功能，而进程服务器则返回倾听新的请求，如图

7-2（b）所示。

不过，有一些服务是独立于进程服务器的，例如，文件服务器需要在特别的硬件（带有磁盘的机器）上运行，不能只是在有人想跟它交流的时候临时建立。

对于这种情况通常使用另一种方案。在这一方案中，有一个特别的进程称作名字服务器，有时也称作目录服务器。为了查找对应一个指定服务名（例如time of day）的TSAP地址，用户建立到达名字服务器的连接（名字服务器在众所周知的TSAP上倾听）。然后，用户发送一个报文指定服务名，名字服务器返回TSAP地址。

接下来，用户释放跟名字服务器的连接，并建立到达所需服务的新连接。该模型要求新的服务建立时，它必须向名字服务器登记，同时给出它的服务名和TSAP地址。名字服务器把这些信息记录在其内部数据库中，一边随后查询到达时，它知道答案。

7.1.3 Internet运输协议TCP

传输控制协议（TCP）通过数据报网络在两个应用层进程之间提供逻辑的全双工（双向）连接。TCP为这些应用进程提供面向连接的可靠的有序的字节流服务。TCP还提供流控制，允许接收方控制发送方传输信息的速率，使得缓冲区不会溢出。TCP也在同一端点系统中支持多个应用进程。

在可以开始传送数据之前，TCP通过设置在协议中使用的变量在两个应用进程之间建立一条连接。这些变量存储在称作传输控制块（TCB）的一个连接记录中。连接一旦建立了，TCP就在连接的每个方向上正确地有序地投递数据。TCP被设计成运行在Internet协议（IP）之上，并且不假定基础网络服务是可靠的。为了实现可靠性，TCP使用一种带选择性重传机制的ARQ。TCP可独立地终止连接的每个方向，在一个方向被关断之后，还允许数据在另一个方向上继续流动。

TCP不保留报文边界，并且把它从应用层得到的数据当作一个字节流处理。因此当一个源在单个块（一次写）中发送一个1000字节的报文时，目的地可能通过2块各500字节（共2次读）接收该报文，也可能以3块的方式（共3次读，分别是400、300和300字节）接收该报文，或者是以其它任意结合的形式接收该报文。换句话说，TCP可以用它认为最适合下层网络的方式分割或结合应用信息。

TCP是在Internet环境中投递面向连接的服务，而Internet本身提供的是无连接的分组传送服务，这样从同一源前往同一目的地的不同分组可能走不同的通路，因此可能不按发送的顺序到达。这样，来自先前的TCP连接的过时的Internet报文可能在现有的TCP连接期间到达接收方，从而使得删除重复报文的任务复杂化。TCP解决这一问题的方法是使用长的（32位）序列号，并且允许在连接建立阶段选择随机的初始序列号。在任一给定时间，接收方从一个小得多的窗口接收序列号，因此接收非常老的报文的可能性是非常小的。此外，TCP在每条连接的端点实施一种超时机制，允许网络清除老的报文段。

发送方把一个连续的字节串安排进一个称作报文段的PDU。报文段包含一个具有地址信息的头，地址信息使网络能够把报文段引向它的目的地应用进程。报文段包含一个序列号，对应在被发送的字节串中的第一个字节的序号。这明显地跟常规的ARQ不同。当在发送缓冲区中的字节数目超过某个指定的门槛时，或当一个被周期性地设置的定时器超时的

时候，发送方就决定发送一个报文段。发送方应用也可以使用一个push命令迫使发送方发送一个报文段。

为了提供带外信令，TCP允许发送者把数据指定成是紧急的，意味着接收程序应被尽可能快地通知紧急数据到达，而不管紧急数据处在流中什么位置。当发现紧急数据时，接收方的TCP便通知与连接相关的应用程序进入“紧急”方式。在所有紧急数据都被消耗完毕之后，TCP又告诉应用程序返回正常运行方式。当在一个报文段中发送紧急数据时用以标志紧急数据的机制由CODE段中的URG位和紧急指针段组成。当URG位置1时，紧急指针（URGENT POINTER）指出窗口中紧急数据结束的位置。紧急指针的值是从序列号段值开始算起的数据段中的正偏移。将紧急指针值与序列号相加就得到最后一个紧急数据字节的编号。

当一个报文段到达时，接收方执行传输错误检查。如果报文段是无错的，并且不是一个重复的报文段，再假定这些字节落入接收窗口之内，那么就把这些字节插入接收缓冲区中适当的位置。需要指出的是，接收方将接受失序的但无错的报文段。

TCP分离流控制功能和应答功能。流控制功能通过在报文段头部的通告窗口段实现。在相反方向传输的报文段包含被通告的窗口大小，它通知发送方在接收方当前可提供的缓冲区的数量。发送方在每次传送一个报文段时，都要设置一个定时器。如果在报文段中还没有一个字节被应答时定时器就超时，那么就重传该报文段。

TCP头中的CHECKSUM（检验和）用于头和数据中的所有16位字。检验和也覆盖了在概念上附加在TCP包头前的伪头，该伪头含有源IP地址、目标IP地址、协议标识符和TCP段长。伪头由源和目的地主机在检验和计算期间建立，但不传送。

TCP使用三次握手过程建立连接。进行连接建立的TCP双方通过交换3个报文段来同步顺序号。握手中的第1个报文段可以被识别，因为它在其CODE段中有SYN位置1。第2个报文段将SYN位和ACK位都置成1，表明它应答第1个SYN同时继续握手过程，最后一个握手报文段仅仅是一个应答，只是用以通知目的地双方一致认为连接已经建立。

通常，一台机器上的TCP软件被动地等待握手，另一台机器上的TCP软件发起连接过程。握手过程设计得很周到，使得即使在双方机器试图同时启动连接的情况下也能正常工作。因此，连接的建立可以从任一端起始或者从两端同时启动。一旦连接建成了，数据就可以同等地在两个方向上流动。这里没有主或从的区别。

因为IP不提供任何控制拥塞的机制，所以它依靠高层检测拥塞和采取应对措施。也可以使用TCP窗口机制来控制在网络中的拥塞。TCP拥塞控制的基本思想是让每个发送方仅发送正确数量的数据，保持网络资源被利用但又不会被过载。如果发送方抢占资源，发送太多的分组，网络将经历拥塞。在另一方面，如果TCP发送方太保守，网络又会得不到充分利用。TCP在不会引起网络拥塞的条件下，其发送方可以发送的最大字节数量是用另一个称作拥塞窗口的窗口指定的。为了避免网络拥塞和接收方缓冲区溢出，TCP发送方在任一时间可以发送的最大数据量是通告窗口和拥塞窗口中的最小值。

使用TCP进行通信的两个程序可以使用CLOSE（关断）操作从容地终止对话。在内部，TCP使用一种修改的3次握手关断连接。TCP连接是全双工的，因为我们把种连接看成包含两个独立的流传送，每个方向上一个。当一个应用程序告诉TCP它没有更多的数据要发送时，TCP将关闭在一个方向上的连接。正在发送的TCP为了关掉一条连接上的方向的那一

半，把剩余数据发送完毕，等待接收方对它应答，然后发送一个FIN位置1的报文段，接收方TCP确认这个FIN报文段，并通知自己这一边的应用程序没有更多的数据可提供（例如，使用操作系统的文件结束机制）。

一旦一条连接关掉一个方向，TCP便拒绝再接受这个方向上的数据。同时，数据可以继续在相反方向上流动，直到发送方关掉那个方向的连接为止。当然，即便是连接已经关断了，确认还是继续流回到发送端。当两个方向都已关断时，在每一端点上的TCP软件便删除各自的连接记录。

有时候，非正常条件的出现会迫使应用程序或网络软件断开一条连接。TCP为这样的非正常断连提供了一个重置设施。为重置一条连接，一侧发送一个报文段，将其CODE段中的RST位置1，以此来启动一次终止过程。另一侧立即使连接非正常中止，以此来响应重置报文段。TCP还通知应用程序发生了重置。重置是一种立即的非正常中止，这就意味着在两方向上的传递都立即停止，像缓冲区这样的资源也被释放。

最后，现在使用的TCP软件假定超时是由拥塞引起的，而不是由分组的丢失引起。因此当超时事件发生时，TCP放慢发送速率，发送较少的分组，其思想是减轻网络负荷，消除拥塞。不幸的是，无线传输链路是高度不可靠的，它们在所有的时间内都丢失分组。处理分组丢失问题的适当方法是重传，并且尽快重传。放慢发送速度只会使事情变得更糟。比如说，如果有20%的分组丢失，那么当发送速率是每秒100个分组时，有效吞吐率是每秒80个分组，而当发送速率减慢到每秒50个分组时，有效吞吐率会下降到每秒40个分组。

事实上，当分组在有线网络上丢失时，发送方应该放慢发送速度；而当分组在无线网络上丢失时，发送方应当发送得更快。当发送方不知道是什么样的网络在引起分组丢失时，就很难做出正确的决定。通常从发送方到接收方的通路是异构的，开头100公里可能是在有线网络上，最后1公里可能是无线媒体。现在对超时做出正确的判断就更加困难了，因为它跟引起故障的位置有关。

一种解决方案由Bakne和Badrinath于1995年提出，称作间接TCP，它把TCP连接分裂成两条隔开的连接。第1条连接从发送方到基站，第2条连接从基站到接收方。基站在两个方向上在两条连接之间拷贝分组。在第1条连接上的超时可以放慢发送方的速度，而在第2条连接上的超时则可以加快发送方的速度。其它参数也可以在两条连接上分开调整。

上述方案的缺点是它违反了TCP的语义。由于连接的每一部分都是完全的TCP连接，基站以通常的方式应答每一个TCP报文段。但此时发送方接收到正确应答并不意味着真正的接收方已经收到了该报文段，只是基站收到了它而已。

7.1.4 Internet运输协议UDP

UDP（User Datagram Protocol）采取无连接的方式提供高层协议间的事务处理服务，允许它们互相发送数据报。也就是说，UDP是在计算机上规定用户以数据报方式进行通信的协议。UDP与IP的差别在于，IP对于系统管理的网络软件可以使用，一般用户无法直接使用，而UDP是普通用户可直接使用的，故称为用户数据报协议。UDP必须在IP上运行，即它的下层协议是以IP作为前提的。

既然UDP是一种无连接的数据报投递服务，它就不保证可靠投递。它跟远方的UDP实

体不建立端到端的连接。而只是将数据报送上网络，或者从网上接收数据报。UDP根据端口（Port）号对若干个应用程序进行多路复用，并能利用检验和检查数据的完整性。

与传输控制协议TCP类似，一台计算机上的应用程序和UDP的接口是UDP端口。这些端口用从0开始的数字编号，每种应用程序都在属于它的固定端口上等待来自其它计算机的客户的服务请求。例如SNMP（简单网络管理协议）服务方（又称代理）总是在161号端口上等待远方客户的服务请求。一台计算机只能有一个SNMP代理程序，因为SNMP服务方只能使用161这一个端口号。这个端口号是人们约定好的，它只能为SNMP服务方利用。当某台计算机的客户请求SNMP服务时，它就把请求发到备有这一服务的目标计算机的161号UDP端口。

UDP保留应用程序定义的报文边界，它从不把两个应用报文组合在一起，也不把单个应用报文划分成几个部分。也就是说，当应用程序把一块数据交给UDP发送时，这块数据将作为独立的的单元到达对方的应用程序。例如，如果应用程序把5个报文交给本地UDP端口发送，那么接收方的应用程序就需要从接收方的UDP端口读5次，而且接收方收到的每个报文的大小都和发出的大小完全一样。

一个TCP/IP主机的UDP模块必须具备产生和验证UDP检验和的功能。一个应用程序使用服务时可以选择是否产生UDP检验和，缺省值是需要产生。当IP模块收到一个IP分组并且发现该分组的头部类型（type）段标明为UDP时，它就将其中的UDP数据报传给UDP模块。UDP模块接收由IP模块传来的UDP数据报，并检查UDP检验和。如果检验和是0，就表明发送方没有计算UDP检验和。如果检验和非0，并且检证的结果不正确，则UDP模块必须抛弃该数据报。如果检验和有效（或0），UDP模块就检查该数据报的目标端口号，如果其端口号与本地的一个应用程序被指定的端口号符合，就将数据报中的应用报文放入队列，让那个应用程序来读取。

跟TCP一样，UDP根据IP分组头中的信息作出伪数据报头，跟UDP数据报头和数据一起进行16位的检验和计算。使用伪报头的目的在于验证UDP数据报是否已到达它的正确报宿。领悟这个伪报头的关键是，要认识到正确报宿的组成包括互连网中一个唯一的计算机和这个计算机上唯一的协议端口。UDP报头本身只是确定了协议端口的编号。因而，为验证报宿，发送计算机的UDP要计算一个检验和，这个检验和包括了报宿主机的IP地址，也包括了UDP数据报。在最终目的地,UDP软件使用从运载UDP报文的IP分组头中得到的目标IP地址验证检验和。如果检验和一致，那么数据报确实到达所希望的报宿主机和这个主机内的正确协议口。

对UDP来说，不具备诸如接收保证和避免重复等有序投递功能，故对那些要求数据必须按顺序到达的应用程序，最好采用TCP；或者用户自己想办法解决顺序到达的问题。例如，TFTP（Trivial File Transfer Protocol）作为文件传送协议之一就在应用层做这方面的工作。

UDP在TFTP及Internet的名字服务等应用中使用。在伯克利的UNIX上，UDP也在一些检查网络用户的命令（如rwho等）中使用。Sun Microsystems公司开发的NFS (Network File System)也是在UDP上实现的。由于UDP协议简单，在每个系统中运行时网络负载很轻，故有利于大量数据和实时数据的高速传送。

7.1.5 Internet关于端口号的约定

TCP和UDP都具有端口号，用于标识数据交换的参与者。在接收方，IP协议标识号先于端口号进行检查，而且TCP和UDP对端口号的使用是彼此独立的。这就是说，同一个端口号可以有两种不同的用途，若一个使用它为TCP服务，则另一个还可以将它用在UPP上。

端口号的选择是很严格的，而且受到限制。端口号值0—255都由DOD（美国国防部）分配，它们称为公用的端口号。任何使用这些端口号的应用程序都必须符合相应的已有明确定义的协议。许多操作系统都把这些公用端口号当作一些受保护的固定端口。这些端口号只能被具有特殊操作系统权限的进程使用。剩余的端口号才能被普通的进程使用。

现在我们来看看应用程序是怎样与运输层协议(UDP或TCP)接口的。假定你要发送一个文件到地址为128.6.4.7的计算机。为连接到128.6.4.7，必须指明你要与FTP服务程序通信。这只要说出该服务程序的对应的端口号就可以做到。TCP使用目标主机的IP地址和端口号区别不同的连接。用户程序通常使用或多或少是随机的端口号，但目标主机上等待请求的服务程序必须使用众所周知的固定端口号。

在我们的例子中，为发送一个文件，你将在本地主机启动一个叫“ftp”的程序，它使用本地的一个随机端口号(比如1234)打开一个连接。然而，它将指定21这个众所周知的端口号为目标端口号。这个端口号由FTP服务程序使用。注意，这里引入了两个不同的程序。你在你这一边运行ftp，它从你的终端接受命令，并传给对话的另一方。它跟目标机器上的FTP服务程序对话。FTP服务方程序则从网络连接接受命令，它运行在目的地主机上。还要注意的是，一个连接实际上是由4个数字确定的，包括双方的IP地址和双方的端口号。IP地址放在IP分组的头部，TCP端口号放在TCP报文段的头部。在任一时刻，一个连接的4个数字不能与其它连接的4个数字相同，但只要有1个数字不同就可以了。 例如，一台机器上的两个用户给同一远方计算机传送文件，所建立的两个连接可能是下面的两组参数：IP地址和TCP端口。

连接1

128.6.4.194→128.6.4.7
1234→21

连接2

128.6.4.194→128.6.4.7
1235→21

由于是同样的两台机器，故IP地址相同，又因为都是做文件传送，故另一端都是众所周知的FTP服务程序端口，唯一不同的是用户运行的程序ftp端口号。一旦TCP打开了连接，我们就可以把连接当成简单的导线那样使用，内部细节都由TCP和IP处理。

7.1.6 运输协议的发展

把现有的运输协议用于千兆位网络将面临着一系列的问题需要人们去解决。第一是序列号的问题。在Internet早期，32位序列号循环周期大于1周，对于后来的10Mbps以太网这

个周期降低到157分钟，问题还不大。而对于1Gbps以太网，循环周期只有大约34秒，低于120秒的分组最长存活时间。

第二，计算速度的提高跟不上通信速率的增长。在1970年代，ARPANET运行速度是56kbps,计算机运行速度约为1MIPS。分组大小是1008位， ARPANET每秒可以投递约56个分组，每个分组差不多花18毫秒的时间，在18毫秒的时间内主机可以执行18000条指令。当然实际上可以为每个分组提供9000条指令，剩下50%CPU时间用于做真正的应用计算。

现在1000MIPS主机在千兆位线路上交换1500字节的分组，分组流动速率可达每秒80000个分组。如果保留一半的CPU时间用于应用，1个分组处理必须在6.25微秒内完成。在6.25微秒内1000MIPS主机可执行6250条指令，这个数目仅是ARPANET主机的1/3。而且当代RISC指令所做的工作要比老的CISC指令少，因此情况会变得更糟。结论是计算机可用于协议处理的时间少了，因此运输协议必须简化。

第三，回退N式协议在具有大的带宽延迟乘积的线路上执行效率差。例如，在以1Gbps运行的4000公里线路上来回路程时间是40ms。在此时间内发送方可能发出5M字节，如果发现错误，在被告知之前可能已经是在40ms之后了。如果回退N，发送方重传的不是仅仅坏的分组，而是晚些时候到达的5M字节，显然这是一个很大的浪费。

第四，千兆位线路不同于兆位线路,千兆位线路是延迟受限而不是带宽受限.例如传送1兆比特的文件,在4000公里1Mbps的线路上,传输时间主要受可以发送的位速率制约,而在1Gbps的线路上,RTT是40毫秒,在光纤上发送只需花1毫秒（取决于带宽）的时间。

第五，对于诸如多媒体这样的新的应用，分组到达时间的变化跟平均延迟一样重要，较慢的但均匀的投递通常比抖动性大的投递更为可取。

面对上述挑战或问题，在千兆位网络中的PDU和协议的设计和实现应该主要关注哪些事项？具有什么样的特征？设计千兆位网络协议的基本原则是：追求速度而不是带宽使用的优化。

分组头应包含尽可能少的域，以减少处理时间；这些域还应该足够大，避免新旧序列号混淆，且接收方可以通告足够的窗口空间。它们还必须遵从字边界对准规则，以便易于处理。对于分组头和数据应该分别计算检验和，使得有只对头而不对数据做检验和，并在把数据拷贝到用户空间之前验证头是正确的。最大数据尺寸应该很大，以允许即时面对长的延迟也能做有效的操作；而且数据块越大，总带宽中用于头的比例也越小。现在的1500字节是太小了。另一个宝贵的特征是可以在连接请求中发送常规数量的数据，这样可节约RTT时间。

最后，把协议软件设计工作的重点放到成功的条件下，因为减少处理时间是首要的，而对错误处理的优化则是第二位的。对于软件工作，还应该减少拷贝次数和时间。在理想的情况下，硬件应该把每个入进分组以连续数据块的方式转储到内存，软件用单个块拷贝就可以把分组拷贝到用户缓冲区。

7.2 基本练习题

1. 选择题

在Internet上，计算机通信的基础构筑块是：

a. 端口
b. 服务器
c. 套接口
d. 分组

解答：c。

2. 填空

当在一个TCP报文段中发送紧急数据时，用以标志紧急数据的机制由_____段中的URG位和_____段组成。当URG位置1时，紧急指针指出窗口中紧急数据_____位置。将紧急指针值与_____相加就得到最后一个紧急数据字节的编号。

解答：当在一个TCP报文段中发送紧急数据时，用以标志紧急数据的机制由 CODE段中的URG位和 紧急指针 段组成。当URG位置1时，紧急指针指出窗口中紧急数据 最后 位置。将紧急指针值与 序列号 相加就得到最后一个紧急数据字节的编号。

3. 选择题

在什么条件下可以打开一条TCP连接？

a. 在两个套接字之间当前不存在连接
b. 有足够的资源支持连接
c. 两个应用进程达成一致
d. MTU和缓冲区尺寸相等
e. 序列号匹配

解答：b和c。

4. 选择题

在下列关于UDP的陈述中，哪一句是正确的？

a. UDP使用TCP传输协议
b. 给出数据的按序投递
c. 不允许多路复用
d. 运行主动的流控机制
e. 是面向连接的

解答：没有一句陈述是正确的。

5. 填空

构造套接号后，网络上具有唯一性的_____地址和_____号结合在一起，才构成唯一能识别的标识符。

解答：构造套接号后，网络上具有唯一性的___IP___ 地址和___端口___ 号结合在一起，才构成唯一能识别的标识符。

6. 选择题

通常在Unix主机上，信任主机（trusted host）名可以在什么文件中查到？

a. /etc/hosts
b. /etc/hosts.equiv
c. /etc/resolv.conf
d. /etc/netwoks

解答：b。

7. 填空

在地址方面，UDP报头本身只是确定了协议_____的编号。因而，为验证报宿，发送计算机的UDP要计算一个检验和，这个检验和既包括了UDP数据报，也包括了_____地址。

解答：在地址方面，UDP报头本身只是确定了协议 ___端口___ 的编号。因而，为验证报宿，发送计算机的UDP要计算一个检验和，这个检验和既包括了UDP数据报，也包括了 ___报宿主机IP___地址。

8. 什么是RPC？

解答：RPC是英文“Remote Procedure Call”的缩写，中文含义是“远地过程调用”。它是一种允许在本地主机上的程序调用位于远地机器上的过程的技术。当在机器1上的一个进程调用在机器2上的一个过程的时候，在机器1上的调用进程被挂起，在机器2上执行被调用的过程。调用参数信息从调用方向被调用方传输，过程结果信息从被调用方返回到调用方。

9. 试叙述做RPC（远地过程调用）的实际步骤。

解答：（1）客户调用客户方的承接过程。这是本地过程调用，参数以通常的方式被推进栈。

（2）客户把参数包装在一个报文中，并做系统调用发送该报文。人们把包装参数的操作叫做参数编配。

（3）客户方内核把报文从客户方机器发送到服务器机器。

（4）服务器的内核把分组传递给服务器的承接过程。

（5）服务器的承接过程用解编配了的参数调用被请求的服务器过程。

应答通过在相反方向上的类似的流程返回到客户。

10. 什么是RTP？

解答：RPC是英文“Real-time Transport Protocol”的缩写，中文含义是“实时传输协议”。它是IETF研制的实时传输协议。RTP标准实际上定义了一对协议，即RTP和实时传输控制协议（RTCP）。前者用于多媒体数据交换，后者用于定期发送跟某个数据流相关的控制信息。当在UDP上运行的时候，RTP数据流和相关的RTCP控制流使用相继的运输层端口。RTP数据使用一个偶数端口号，RTCP控制信息使用下一个较高的（奇数）端口号。

11. RTP的设计提出了一个什么样的机制？

解答：因为RTP被设计成支持广泛种类的应用，它提出了一个灵活的机制，使得在研制新的应用的时候不必反复修改RTP协议本身。对于每个种类的应用（例如音频），RTP定义一个预制文件和一个或多个格式。该预制文件提供一个范围的信息，以保证在该类应用中对RTP头的各个段有共同的理解。格式描述说明如何解释后随RTP头的数据。例如，RTP头可能后随一个字节序列，每个字节代表单个音频采样，该采样跟前一个采样有规定的时间间隔。数据格式也可能比较复杂，例如，使用MPEG编码的视频流就需要有大量的结构表示所有不同类型的信息。

12. RTP的设计包含了一个什么样的体系结构原则？

解答：RTP的设计包含一个称作应用级成帧（ALF）的体系结构原则。该原则是由Clark和Tennenhouse 在1990年提出来的一个为正在涌现的多媒体应用设计协议的新方法。他们意识到，现存的协议，如TCP，不太可能很好地服务于这些新应用，而且也不可能有一个通用的协议满足所有这些新应用的需求。该原则的核心是相信应用程序本身最了解自己的需要。例如，一个MPEG视频应用最懂得如何从丢失的帧中恢复，以及如何对I帧或B帧的丢失做出不同的反应。同样的应用也懂得如何将待传输的数据分段，例如，最好把来自不同帧的数据放在不同的数据报中发送，以便一个丢失的分组仅破坏单个帧，而不是两个帧。正因为这个原因，RTP把许多协议细节都放到预制文件和格式文档中，而且这些细节都是针对一个应用的。

13. RTP提供哪些服务？它位于OSI 七层协议模型中的哪个层次？

解答：RTP为实时数据（例如音频、视频等）提供端到端的服务，这些服务包括：负载类型标识、顺序编号、时间定位和传输监控等。然而，RTP本身并不提供对信息传输的任何时间和质量上的保证，而是依赖其下层网络提供这样的功能。同时，它既不保证传输的可靠性，也不假定下层网络能提供可靠的和保序的通信。RTP分组中的顺序号使接收方按顺序重组信息成为可能。如果把RTP和RSVP协议配合使用，就可以为在Internet上传输多媒体数据提供一个切实可行的解决方案。

典型的RTP运行在UDP之上，在层次结构上，我们也可以认为RTP和UDP共同完成运输层的功能，然而RTP亦可基于其它各种运输层和网络层，如果下层网络许可，RTP可支持广播数据传输。

14. 如图7-3所示，一支白色部队在山谷里扎营，在周围的两边山坡上都驻扎着兰色部

队。白色部队比两支兰色部队中的任一支都要大，但两支兰色部队加在一起就要比白色部队大。如果一支兰色部队单独作战，那么它就会被白色部队击败。但若两支兰色部队同时进攻，他们将能够把白色部队战败。两支兰色部队需要同步他们的进攻。然而，他们唯一的通信媒介是步行进入山谷，而在那里他们有可能被俘虏，从而将信息丢失（也就是说，他们必须使用非可靠的通信信道）。问题是，是否存在一个协议，能够使得兰色部队取胜？

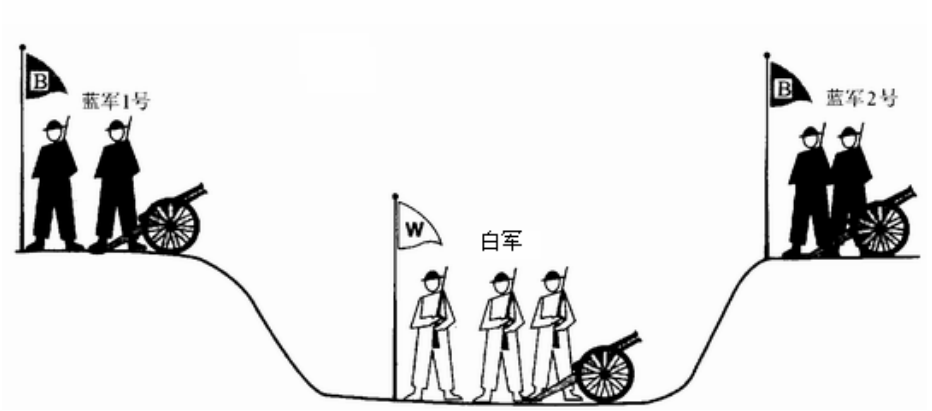


图 7-3　两军问题

解答：假定第一支蓝色部队的司令员发送一个报文说：“我建议我们在3月29日黎明进攻，怎么样？”现在假定报文传到了，第二支兰色部队的司令员同意所提出的建议，并且他们的回答也安全地到达第一支蓝色部队。那么，联合进攻会发生吗？有可能不会，因为第二支兰队的司令员不知道他的应答是否到达对方。他知道，如果他的回答到达不了，那么第一只兰队不会举行进攻。在这种情况下，他自己单独命令进攻将是愚蠢的。实际上，不存在一个协议能够使得蓝色部队取胜。

15. 选择题

通常在Unix主机上，下列哪一个文件允许一个远程用户不用给出口令就可以登录到本地另一个用户的目录中？

a. /etc/rc
b. /etc/hosts
c. .rhost
d. /etc/exports

解答：c。

16. 在Unix系统中，运输层的协议号和服务方应用程序的端口号分别在哪两个文件中定义？

解答：在Unix系统中，运输层的协议号和服务方应用程序的端口号分别在/etc/protocols和/etc/services中定义。

17. 为什么要使用UDP？让用户进程直接发送原始的IP分组不就足够了吗？

解答：仅仅使用IP分组还不够。IP分组包含IP地址，该地址指定一个目的地机器。一旦这样的分组到达了目的地机器，网络控制程序如何知道该把它交给哪个进程呢？UDP分组包含一个目的地端口，这一信息是必需的，因为有了它，分组才能被投递给正确的进程。

7.3 综合应用练习题

1. 在Internet文件服务器和客户访问的套接口编程中，要求两部分程序中的SERVER_PORT值必须相同。这一点很重要，为什么？

解答：如果客户发送一个分组给SERVER_PORT，而服务器没有在那个端口上倾听，那么分组将不会投递给该服务器。

2．数据报的分片和重组由IP控制，并且对于TCP不可见。这是不是意味着TCP不必担心到达数据的失序问题？

解答：尽管到达的每个数据报都是完整的，但可能到达的数据报顺序是错误的，因此，TCP必须准备适当地重组报文的各个部分。

3．在主机1上的一个进程被分配端口p，在主机2上的一个进程被分配端口q。试问，在这两个端口之间是否可以同时有两条或更多条TCP连接？

解答：不可以。一条连接仅仅用它的套接口标识。因此，（1，p）----（2，q）是在这两个端口之间唯一可能的连接。

4. UDP和TCP都使用端口号标识报文投递的目的地实体。至少给出两条理由，说明这些协议为什么要采用一个新的抽象ID（端口号），而不使用在设计这些协议时就已存在的进程ID？

解答：这里有三个理由。首先，进程ID是操作系统特有的，使用进程ID将使得这些协议依赖于操作系统。第二，单个进程有可能建立多个通信通道，把单个进程ID用作目的地标识符不能够对这些通道互相区别。第三，让进程在周知口上倾听是可能的，但周知的进程ID是不可能的。

5．在表7-3示出的样例运输层原语中，LISTEN是一个封锁性调用。这样做严格地讲是必需的吗？如果不是，请解释可以怎样使用一个非封锁原语，并说明较之封锁方案有什么优点。

表7-3　习题2中的样例运输层原语

原　　语	发送的TPDU	含　　义
LISTEN	（无）	封锁，直至某个进程尝试连接
CONNECT	CONNECTION REQ.	主机尝试建立连接
SEND	DATA	发送信息
RECEIVE	（无）	封锁，直到一个DATA TPDU 到达
DISCONNECT	DISCONNECTION REQ.	一边要释放连接

解答：不是。事实上，LISTEN 调用可以表明建立新连接的意愿，但不封锁。当有了建立连接的尝试时，调用程序可以被提供一个信号。然后，它执行，比如说，OK或REJECT来接受或拒绝连接。然而，在原先的封锁性方案中，就缺乏这种灵活性。

6．图7-4示出了使用在习题5中给出的运输原语的连接建立和释放的状态图。实线表示客户端的状态序列，虚线表示服务器端的状态序列。在该图中我们假定分组可能被网络层丢失，因此必须逐个确认。现在假定网络层是百分之百地可靠，什么时候都不会丢失分组。那么，需要对图7-4作什么样的修改？

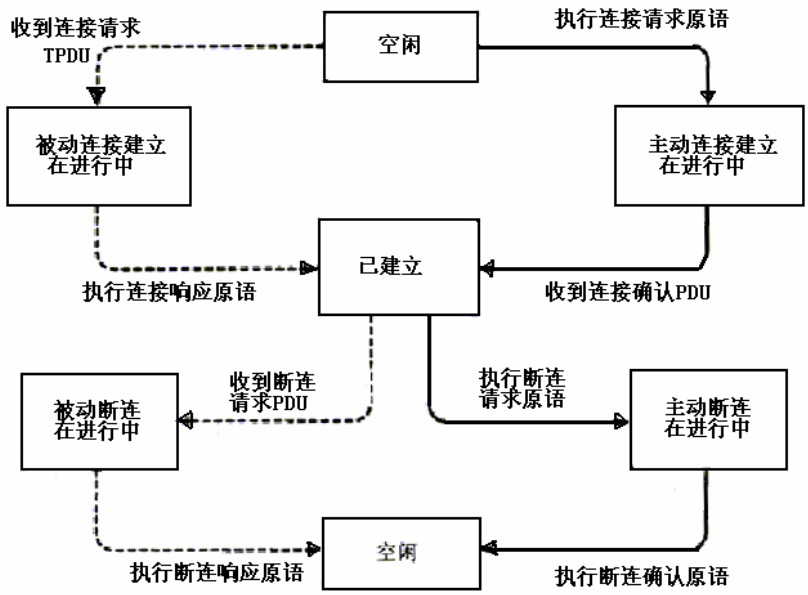


图 7-4　运输连接建立和释放状态图

解答：从“被动连接建立在进行中”到“已建立”的虚线不再依确认的传输情况而定。该变迁可立即发生。实质上，“被动连接建立在进行中”状态已经消失，因为它们什么时候都不可见。

7. 假定使用时钟驱动方案产生初始序列号，时钟计数器的长度是15位。时钟每100毫秒滴答一次，最大的分组存活期是60秒。问需要多长时间进行一次再同步？

（a）考虑最坏情况

（b）在数据每分钟消耗240个序列号的情况下

解答：在具体地解答这个问题之前，需要先熟悉一下时钟驱动方案的内含。首先我们引入参数T，假定在发送出一个分组之后等待长度等于T的时间，我们就可以肯定，所有关于该分组的踪迹都已消失，不管是该分组本身，还是对于它的确认都不会再意外地出现。我们还假定，每个主机都配有一个表示一天的时间的时钟，不同主机上的时钟不必同步。每个时钟都采用二进制计数器的形式，并且以长度一致的间隔时间递增。而且，计数器的比特数必须等于或超过序列号所使用的比特数。最后一点，时钟被假定是连续运行，即使主机关闭时也不间断。

时钟驱动方案的基本思想是同一时间不会有两个活动的TPDUs使用相同的序列号。在一条连接建立的时候，时钟的低端k个比特被用作初始序列号（也是k位）。因此，每条连接可以从不同的序列号开始为TPDU编号。序列号空间应该足够大，使得当编号循环一周时，具有相同号码的旧的TPDU已经不复存在。

当主机系统崩溃时会产生一些问题。在重新启动后，主机的运输层实体不知道它曾经处在序列号空间的什么位置。一种解决办法是要求运输层实体在恢复后的T秒内处于空闲状态，让所有老的TPDUs都消失。然而，在一个复杂的互连网上，T值可能很大，所以这不是一个好的解决办法。

为了避免从崩溃恢复后的T秒不工作状态，需要对序列号的使用施加新的限制。如图7-5所示，在一些编号可能被用作初始序列号之前，必须在长度为T的时间内禁止使用这些编号。在图7-5（a）中，我们把禁止的时间和序列号的结合称作禁止区。在任何连接上发送TPDU之前，运输层实体必须读一次时钟，检查该TPDU的编号是否在禁止区内。

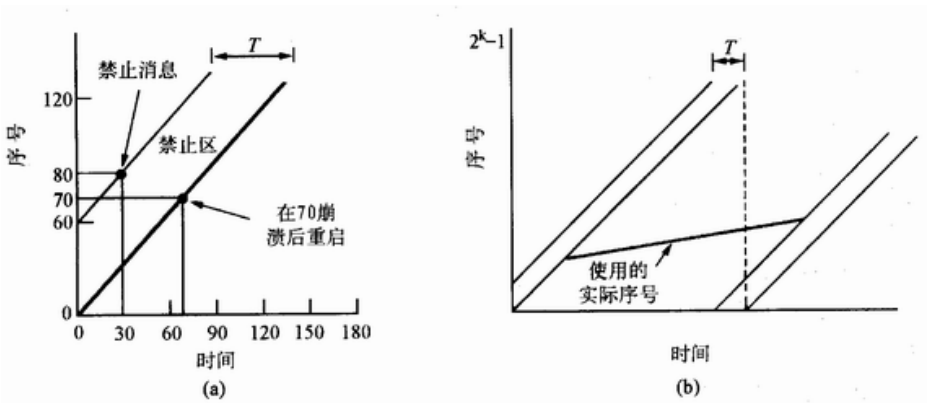


图 7-5　（a）不让 TPDU 进入禁止区　（b）重新同步问题

显然，在任何连接上的最大数据速率是每个时钟滴答发送一个TPDU。在系统崩溃后重启动时，在打开一条新的连接之前，传输实体必须等待到下一个时钟滴答，以避免同样的号码重复使用。从7-5（b）可以看出，如果数据速率低于时钟速率，实际使用的序列号对于时间的曲线将最终从左边进入禁止区。如果这样的情况发生了，要么延迟TPDU达T长度时间，或者重新同步序列号。作为例子，如果在坐标起点发1号TPDU，到接近时钟大循环编码的末尾才发送第2个TPDU，此时为避免在下一大循环开始重复使用序列号，就需要在

大循环接近末尾处重新同步，使用大的初始序列号，以避免使用禁止区号码。

（a）时钟大循环周期是2^{15}，即32768滴答，每滴答100毫秒，即0.1秒，所以大循环周期是3276.8秒。假定数据产生速率非常低（接近零），那么发送方在3276.8-60=3216.8秒时进入禁止区，需要进行一次重新同步。

（b）每分钟使用240个序列号，即每秒使用4个号码，如果时间以t表示（以秒为单位），那么实际的序列号是4t。如图7-5（b）所示，当接近大循环的末尾时以及在下一大循环的开始阶段，4t有一定的大小，位于禁止区的上方。现在由于每秒钟10个滴答，禁止区的左边是10（t-3216.8）。令4t=10（t-3216.8），得t=5316.3（秒）。即当t=5316.3秒时，开始进入禁止区，因此当t=5316.3秒时需要进行一次重新同步。

8. 最大分组存活时间T必须足够地长，保证不仅数据分组，而且确认应答都已消失。请说明为什么？

解答：首先看图7-6所描述的三次握手过程是如何解决延迟的重复到达的分组所引起的问题的。在图（a）中，当主机1发出连接请求时，主机1选择一个序号x，并向主机2发送一个包含该序号的请求TPDU；接着，主机2回应一个接受连接的TPDU，确认x，并声明自己所选用的初始序列号y；最后，主机1在其发送的第一个数据TPDU中确认主机2所选择的初始序列号。图（b）说明当出现延迟的重复的控制TPDU时，三次握手方法是如何工作的。第一个TPDU是来自于一个已经释放的连接的延迟重复的连接请求（CONNECTION REQUEST），该TPDU在主机1毫不知晓的情况下到达主机2。主机2通过向主机1发送一个接受连接的TPDU（CONNECTION ACCEPTED）来响应该TPDU，而该接受连接的TPDU的真正目的是要证实主机1确实试图建立一个新的连接。在这一点上，关键在于主机2建议使用y作为从主机2到主机1交通的初始序列号，从而说明已经不存在包含序列号为y的TPDU，也不存在对y的应答分组。当第二个延迟的TPDU到达主机2时，z被确认而不是y被确认的事实告诉主机2这是一个旧的重复的TPDU，因此废止该连接过程。在这里，三次握手协议是成功的。

最坏的情况是延迟的“连接请求”和对“连接被接受”的确认应答都在网络上存活着。可以设想，当第2个重复分组到达时，如果在网上还存在一个老的对序列号为y的分组的确认应答，显然会破坏三次握手协议的正常工作，故障性地产生一条没有人真正需要的连接，从而导致灾难性的后果。

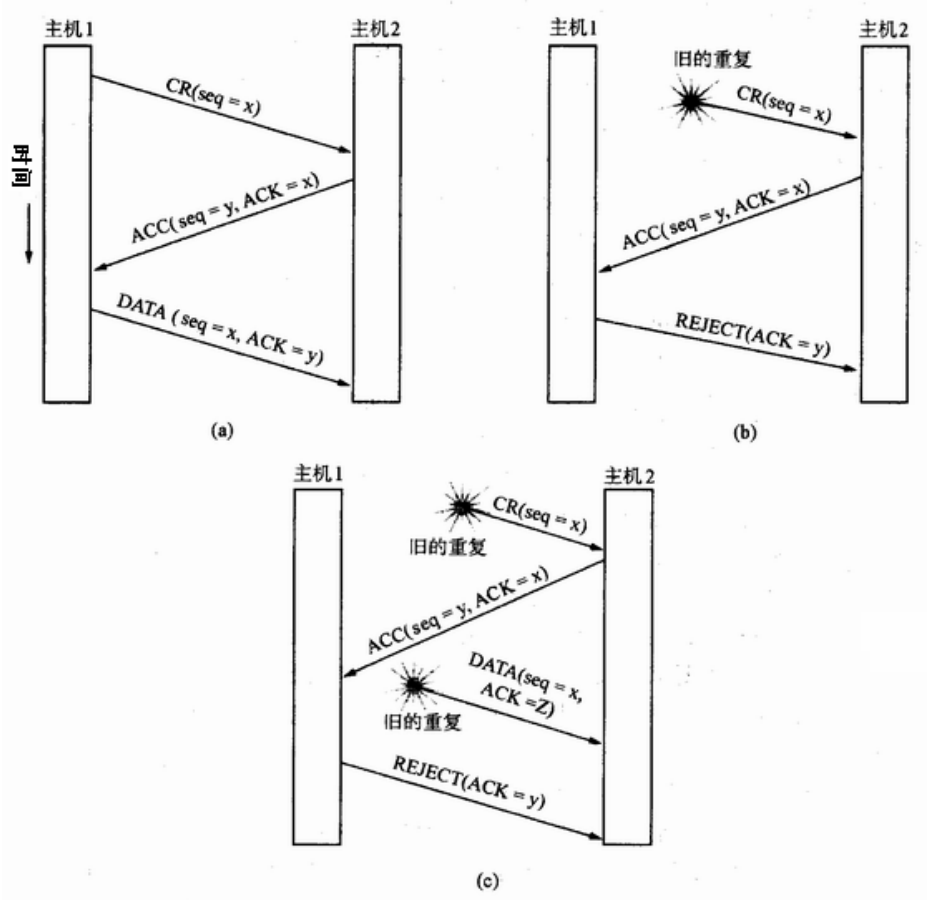


图 7-6　使用三次握手建立连接的协议过程

9. 假定使用两次握手替代三次握手来建立连接。也就是说，不需要第三个报文。那么现在是否可能产生死锁？请给出例子来说明你的答案。

解答：我们知道，3次握手完成两个重要功能，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与确认。

现在把三次握手改成仅需要两次握手，死锁是可能发生的。作为例子，考虑计算机A和B之间的通信。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用于A到B的交通，也不知道A是否同意B所建议的用于B到A交通的初始序列号，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，只等待接收连接确认应答分组。而A在发出的分组超时后，重复发送同样的分组。这样就形成了死锁。

10. 考虑一个简单的应用级协议，它建立在UDP上，允许客户检索一个驻留在周知的地址上的远程服务器上的一个文件。客户首先发送一个带有文件名的请求，服务器用一系列数据分组应答，包含被请求文件的不同部分。为保证可靠性和有序投递，客户和服务器使用停-等协议。忽略明显的性能问题，你看这个协议有什么问题吗？请仔细考虑处理崩溃的可能性。

解答：客户有可能得到错误的文件。假定客户A发送一个对文件f1的请求，然后崩溃。接下来另一个客户B跟A在同一台机器上运行（具有同样的IP地址），并且把它的UDP套接口绑定到跟先前的客户A使用的端口相同的端口。如果客户B的请求丢失了，当服务器对A的请求的应答到达时，客户B将接收它，并把它看成是对他自己的请求的应答。

11. 考虑从主机崩溃恢复的问题（参见图7-7），如果在对输出进程的写操作和发送确认应答之间的间隔时间（或者在发送确认应答和对输出进程的写操作之间的间隔时间）可以做得相对地小，那么，为了减少协议失败的可能性，最好的发送方-接收方策略是什么？

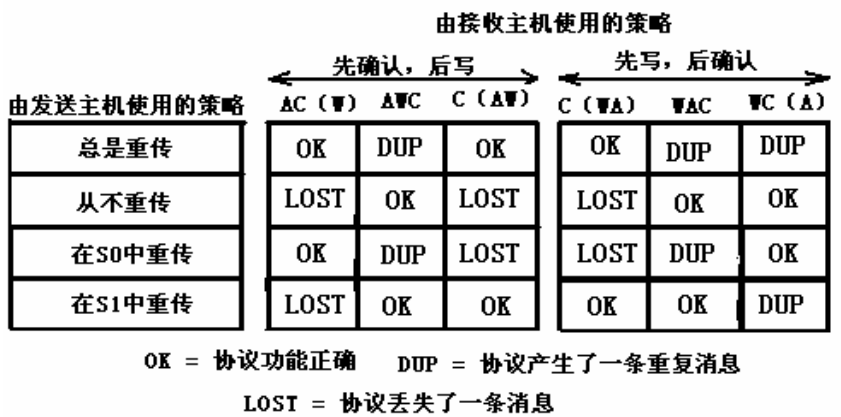


图 7-7　客户机和服务器策略的不同组合

解答：在解答本习题之前，让我们先考察主机从崩溃恢复所带来的问题。我们总是希望，在服务器崩溃随后很快又重新引导的情况下，客户机能够继续工作。为了说明这一问题的难度，我们假定一个客户主机发送一个长文件给另一个服务器主机，并且使用简单的停-等协议。在服务器上的运输层只是简单地把收到的TPDU一个一个地递交给传输用户。假定在文件传输的过程中，服务器崩溃了。当服务器恢复的时候，它的表被重新初始化，因此再也不知道崩溃前文件传送进展到什么地方了。

在试图恢复先前状态的过程中，服务器可能发送一个广播到所有其它主机，宣布自己刚刚发生了一次崩溃，请求客户告知所有打开的连接的状态。此时，每个客户机都可能处于二中择一的状态：有一个悬而未决的TPDU的S1状态，或者没有未确认应答的TPDU的S0状态。可以想到的一种解决方案是基于这一状态信息，客户机决定是否要重发最近的一个TPDU。

乍看起来，这一解决方案似乎能解决问题，可是深入仔细地分析一下，困难仍然很大。作为示例，假定服务器的运输层实体先发送ACK，在ACK被发出之后，再执行把收到的

TPDU写到应用进程的操作。把TPDU写到输出设备和发送ACK是两个不同的事件，不能同时进行。如果服务器主机的崩溃刚好发生在应答被发送之后，并且是在写操作之前，那么客户机将接收到确认应答，当崩溃恢复通告到达时会处于状态S0。因此，客户机不会重传TPDU，错误地认为服务器成功地收到并存放好了它最后一次发送的TPDU。实际的情况并非如此，从而结果是丢失了最后一个TPDU。

到此，你也许会想：“这个问题容易解决，只要你重新编写程序，让传输实体先执行写操作然后再发送ACK就可以了。”可是，写操作尽管成功了，但崩溃可能发生在发送出ACK之前。此时客户机将会处于状态S1，因而重新发送，导致对服务器的应用进程的输出中产生未检测到的重复TPDU。

如图7-7所示，服务器可以选择两种方式中的一种：先确认应答，或者先执行写操作。客户机可以选择四种方式中的一种：总是重传最后一个TPDU，永不重传最后一个TPDU，仅在S0状态时重传，或者仅在S1状态时重传。这样就存在8种可能的组合，但可以看出，对于每一种组合，都有一些事件会使协议的运行失败。

在服务器方可能发生三种事件：发送一个ACK（A），对输出进程的写操作（W）和系统崩溃（C）。三种事件可能以6种不同的次序发生：AC（W），AWC，C（AW），C（WA），WAC和WC（A），这里的圆括号表示，在系统崩溃C后，A和W事件就不可能了。图7-7示出了客户机和服务器的策略的所有8种组合，以及对于每一种组合的有效事件序列。值得注意的是，对于每一种策略都存在某些事件会引起协议失败。例如，如果客户机选择总是重发送，AWC事件将产生检测不出来的收到重复分组的错误，尽管对于C（AW）和C（WA）该协议都工作得很好。

现在我们再回答本道习题的答案。如果AW或WA间隔时间很短，事件AC（W）和WC（A）就不太可能发生。此时的最好发送方策略是，如果崩溃恢复时处于状态S1，应该重传最后一个TPDU，接收方采用顺序AW或WA则无关紧要。

12．（a）阅读下面描述的一个运输层实体的协议规范，理解其中所使用的运输层运行机制。

有一个运输层实体使用面向连接的可靠的网络层服务。它被设计成用户进程的一部分，当用户执行诸如LISTEN这样的封锁性运输原语时，整个传输实体也都被封锁。对网络层的接口是通过过程to_net 和from_net实现的。每一个过程调用都有6个参数，它们包括跟网络层虚电路一对一映射的连接标识符，表示控制报文的Q比特，表示在下一个分组中有该报文的更多数据的M比特，表示六个分组类型中的一个类型的分组类型（六个类型是CALL REQUEST，CALL ACCEPTED，CLEAR REQUEST，CLEAR CONFIRMATION，DATA 和CREDIT），指向数据段的一个指针，以及给出数据字节的数目的一个整数。

在调用to_net时，运输层实体填写准备让网络层读取的所有参数；在调用from_net时，网络层把一个接收到的运输层分组递交给运输层实体。通过传递过程参数信息，而不是传递实际的外出或进入的分组本身，这样传输实体就用不着了解网络层协议的细节。如果传输实体试图在下层的虚电路滑动窗口已满的时候发送一个分组，它将在to_net内被挂起，直到在窗口内有空间为止。这种机制对传输实体透明，并且由网络层使用enable_transport_layer 和disable_transport_layer 这类命令控制。网络层窗口的管理由网络层

负责执行。

除了上述透明的挂起机制，传输实体还可以调用明确的sleep 和wakeup过程。当传输实体被逻辑上封锁等待一个外部事件发生的时候（通常是一个分组的到达），调用过程sleep(休眠)。在调用sleep之后，传输实体（和用户进程）停止执行。

每条传输连接总是处于七种状态之中的一种状态。这七种状态是：

（1）IDLE（空闲）------连接尚未建立。
（2）WAITING（等待）------已经执行CONNECT，送出了CALL REQUEST。
（3）QUEUED（排队）------到达了一个CALL REQUEST，还没有LISTEN。
（4）ESTABLISHED（已建立）------连接已经建立。
（5）SENDING（发送）------用户等待发送分组的许可。
（6）RECEIVING（接收）------已经做了RECEIVE调用
（7）DISCONNECTING（断连）------本地已做了DISCONNECT。

当发生下列三种事件中的任一事件时，都会产生状态变迁：

（1）执行一个原语
（2）有一个分组到达
（3）超时

大多数过程都是用户程序可直接调用的，但packet_arrival 和clock除外。它们是由外部事件自动触发的，分别由分组的到达和时钟滴答期满引起。事实上，它们都是中断性例程。我们假定，当传输实体的过程正在执行的时候，它们不会被调用。仅当用户进程处于休眠状态，或用户进程在传输实体的外部执行时，才可以调用这两个过程。这一性质对于传输实体功能的正确实现是至关重要的。

普通的数据报文以Q=0发送分组。在我们的例子中，仅有一个CREDIT是传输协议控制报文，它以Q=1的数据分组格式发送。控制报文由接收方传输实体检测和处理。

传输实体使用的主要数据结构是数组conn，对应每个潜在的连接都有一个记录。记录维持连接的状态，包括在每一端的传输地址，在该连接上发送和接收的报文的数目，当前状态，用户缓冲区指针，到目前为止当前报文发送或接收的字节数，表示远方用户已发出DISCONNECT的一个比特，一个计时器，用以允许发送报文的允许计数器。每个conn登录项的初始状态都设置成IDLE。

当用户调用CONNECT的时候，网络层被指令发送CALL REQUEST 分组给远方的机器，用户被置成睡眠态。当CALL REQUEST分组到达另一边时，那里的传输实体被中断，运行packet_arrival 检查本地用户是否在指定的地址倾听。如果在倾听，就发回一个CALL ACCEPTED分组，并唤醒远方用户。如果那儿的本地用户不在倾听，就将CALL REQUEST放入队列，等待TIMEOUT。如果在超时前做了LISTEN，连接将被建立，否则发生超时事件，并以CLEAR REQUEST分组拒绝连接。

该传输协议使用了一种不同于传统的滑动窗口的流控机制。当用户调用RECEIVE 时，就向发送方机器上的传输实体发送一个特别的credit报文，并记录在conn数组中。当调用SEND时，传输实体检查在指定的连接上是否有credit到达。如果有，就发送报文（可以是

多个分组），并减少credit；如果尚无credit到达，传输实体就让自己进入睡眠态，直到有一个credit到达。这种机制保证只有当对方已经做了RECEIVE之后，才能够发送报文。这样做的结果是，每当有一个报文到达时，保证有存放它的缓冲区空间可用。总起来讲，该机制允许接收方提供多个缓冲区和请求多个报文。

（b）对于在上面描述的传输实体会产生死锁吗？

解答：该传输实体有可能死锁。当双方同时执行RECEIVE 时就会进入死锁状态。

13. 出于好奇，在习题12（a）中叙述的传输实体的实现者决定在sleep过程的内部放置一些计数器，收集关于conn数组的统计信息。在这些信息当中有七种可能的状态（Queued, listening, waiting, established, disconnecting, sending, receiving）中的每一种状态的连接数目，即n_i (i=1,…,7)。在编写出大块的FORTRAN程序分析数据之后，我们的实现者发现看来关系式Σn_i = MAX_CONN总是成立。仅就这七个变量而言，是否还有其它的恒定关系式？

解答：有，$n_2+n_3+n_6+n_7=1$

因为状态listening(n_2)、waiting(n_3)、sending(n_6) 和 receiving(n_7)都意味着用户被封锁，因此当处在其中的一个状态时，就不可能是在另一个状态。

14. 当在习题12（a）中描述的传输实体的用户发送一个长度为零的报文时将会发生什么情况？请讨论你的回答的意义。

解答：长度为零的报文被另一边接收。这种报文的发送可以被用来表示文件结束的信号。

15. 对于在习题12（a）中描述的传输实体，当用户休眠在sending状态时，说明每一个可能发生的事件是否是合法的。

解答：因为用户处于封锁状态，所有的运输层原语都不可能执行。因此，仅分组到达事件是可能的，而且还不是所有的到达事件。事实上，仅仅跟呼叫请求、清除请求、数据分组和信用量分组这几个分组到达有关的事件是合法的。

16．讨论信用量协议相对于滑动窗口协议的优点和缺点。

解答：滑动窗口协议比较简单，仅需要管理窗口边缘一组参数，而且，对于到达顺序有错的TPDU不会引起窗口增加和减少方面的问题。然而，信用量方案比较灵活，允许独立于确认，动态地管理缓冲区。

17．一个TCP报文段的最大载荷是65495字节，为什么要选择这样一个奇怪的数字呢？

解答：整个TCP报文段必须适配IP分组65515字节的载荷段。因为TCP头最少20个字节，所以仅剩下65495字节用于TCP数据。

18．给出Nagle算法用于严重拥塞网络潜在的缺点。

解答：Nagle算法建议，当数据一次一个字节地来到发送方时，只发送第一个字节，并且缓冲所有其它内容，直到所发出的字节被确认为止。然后在一个TCP报文段中发送所有缓冲的字符。接着又开始缓冲，直到前一个报文段中的所有字节又被确认。这样，如果用

户键入的速度足够快，而网络比较慢的话，那么在每个报文段中都可以有相当数量的字符。该算法还允许输入足够的数据以填满半个窗口或一个最大报文段的情况下发送一个新的分组。在这种运行方式下，尽管用户是以均匀的速度键入，而字符却是以突发的方式回印。用户可能敲击了好几个键，而屏面上什么都没有显示，然后突然地在屏面上显示出所有已键入的字符。人们可能对此感到恼火。

19．一台TCP机器在1Gbps的通道上使用65535字节的发送窗口，单程延迟时间等于10毫秒。问可以取得的最大吞吐率是多少？ 线路效率是多少？

解答：10毫秒×2=20毫秒

每20毫秒可以发送一个窗口大小的交通量，每秒50个窗口（1000毫秒÷20毫秒=50）

65535×8×50 = 26.214Mbps

26.214Mbps÷1000Mbbps ≈ 2.6%

所以，最大吞吐率是26.214Mbps，线路效率约为2.6%。

20．图7-8示出了TCP连接管理的有限状态机。其中粗实线是客户机常规通路。粗断续线是服务器的常规通路。细线是非常事件。试叙述进入SYN RCVD 状态的两个途径。

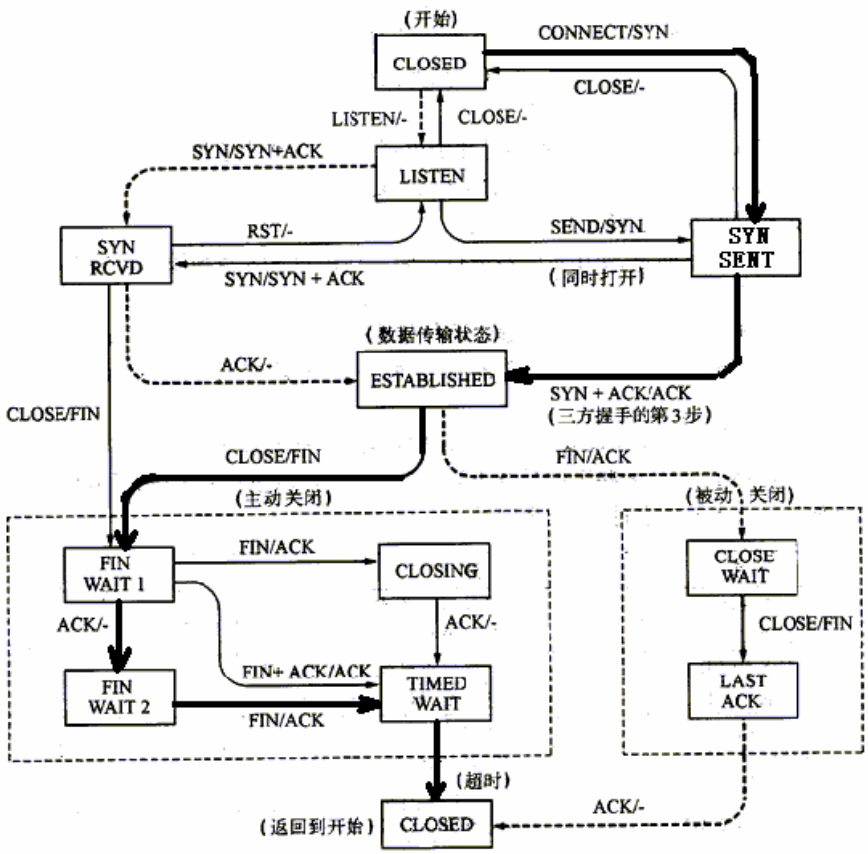


图 7-8　TCP 连接管理的有限状态机

解答：一条途径是从LISTEN 开始。如果收到一个SYN，那么协议进入SYN　RECD

状态。另一条途径是一个进程试图做一个主动打开操作，并发送一个SYN。如果另一方也在做打开操作，并收到一个SYN，那么也将进入SYN RECD状态。

21．考虑在一条具有10毫秒来回路程时间的线路上采用慢启动拥塞控制而不发生网络拥塞情况下的效应。接收窗口24KB，且最大段长2KB。那么，需要多长时间才能够发送第一个完全窗口？

解答：慢启动拥塞控制考虑了两个潜在的问题，即网络容量和接收方容量，并且分别处理每一个问题。为此，每个发送方都维持两个窗口，即接收方准许的窗口和拥塞窗口。发送方可以发送的字节数是这两个窗口中的最小值。

当建立一条连接的时候，发送方把拥塞窗口初始化为在该连接上使用的最大报文段尺寸。然后它发送一个最大报文段。如果这个报文段在超时之前得到确认，发送方就把拥塞窗口增加到两个最大报文段长，并发送两个报文段。当发出去的每个报文段被确认时，拥塞窗口都要增加一个最大报文段长。因此，当拥塞窗口是n个报文段时，如果所有n个报文段都及时得到确认，那么拥塞窗口将增加相当于n个最大报文段的字节数。事实上，每一次突发性连续报文段都会使拥塞窗口加倍。

拥塞窗口继续按指数型增长，直到超时发生，或者到了接收方窗口的边界。其思想是如果突发量1024、2048和4096字节工作得很好，但8192字节的突发量引起超时，那么拥塞窗口应该设置成4096以避免拥塞。只要拥塞窗口保持在4096，不管接收方准许什么样的窗口空间，都不会发送大于4096字节的突发量。这种算法就被称为慢启动。当然，它根本不是慢的意思。现在所有的TCP实现都需要支持这个算法。

现在，最大的段长是2KB，开始的突发量分别是2K，4K，8K和16K字节，下面是24KB，即第一个完全窗口。10毫秒×4=40毫秒

因此，需要40毫秒才能发送第一个完全窗口。

22．假定TCP拥塞窗口被置成18K字节，并且发生了超时事件。如果接着的4个突发量传输都是成功的，那么该窗口将是多大？假定最大报文段长度是1KB。

解答：在Internet的拥塞控制算法中，除了使用慢启动的接收窗口和拥塞窗口外，还使用第3个参数，即门槛值，开始置成64K。当发生超时的时候，该门槛值被设置成当前拥塞窗口值的一半，而拥塞窗口则重置成一个最大报文段长。然后再使用慢启动的算法决定网络可以接受的突发量，一直增长到门槛值为止。从这一点开始，成功的传输线性地增加拥塞窗口，即每一次突发传输后只增加一个最大报文段，而不是每个报文段传输后都增加一个最大报文段的窗口值。

现在由于发生了超时，下一次传输将是1个最大报文段，然后是2个、4个和8个最大报文段，所以在4次突发量传输后，拥塞窗口将是8K字节。

23．如果TCP来回路程时间RTT的当前值是30毫秒，随后应答分别在26、32和24毫秒到来，那么新的RTT估算值是多少？假定 $\alpha = 0.9$。

解答：对于每一条连接，TCP都维持一个变量RTT，它是当前到达目的地的最佳估计值。当发送一个报文段的时候，启动计时器，查看应答要化多长时间，如果时间太长，就

要重发报文段。如果应答在超时前返回，TCP就测量应答化了多长时间，比如说是M，然后用下列公式更新RTT值：

RTT = α RTT + （1 – α）M

现在α=0.9， RTT = 30毫秒 M1=26， M2=32， M3=24
所以，RTT1 = 0.9×30 +（1-0.9）×26 = 29.6
RTT2 = 0.9×29.6 +（1-0.9）×32 = 29.84
RTT3 = 0.9×29.84 +（1-0.9）×24 = 29.256
因此，新的RTT估算值分别是29.6毫秒、29.84毫秒和29.256毫秒。

24．在一个网络中，最大TPDU尺寸为128字节，最大的TPDU存活时间为30秒，使用8位序列号，问每条连接的最大数据速率是多少？

解答：具有相同编号的TPDU不应该同时在网络中传输，必须保证，当序列号循环回来重复使用的时候，具有相同序列号的TPDU已经从网络中消失。现在存活时间是30秒，那么在30秒的时间内发送方发送的TPDU的数目不能多于255个。

255×128×8÷30 = 8738 bps

所以，每条连接的最大数据速率是8.738kbps。

25．一个客户机通过1千兆位/秒的光缆发送128字节的请求给位于100公里以外的服务器。在该远地过程调用期间线路的效率如何？

解答：128字节等于1024位，在1Gbps的线路上发送1000位需要1微妙的时间。光在光导纤维中的传播速度是每毫秒200公里，请求到达服务器需要传输0.5毫秒的时间，应答返回又需要0.5毫秒的传输时间。总起来看，1000位在1毫秒的时间内传输完成。这等效于每秒1兆位，即线路效率是0.1%。

26．再考虑上一道练习中的问题，试计算对于1Gbps和1Mbps的最小可能的响应时间。你可以得到什么样的结论？

解答：在1Gbps，响应时间由光的速度决定。可以取得的最好情况是1毫秒。在1Mbps，发射1024位需要大约1毫秒的时间，再经过0.5毫秒最后一位到达服务器，还需要另外0.5毫秒应答才能返回，这是最好的情况。因此，最好的RPC时间是2毫秒。结论是，线路速度改善到1000倍，性能仅改善到2倍。对于这种应用，除非千兆位线路特别便宜，否则是不值得拥有的。

27．假定你测量接收一个TPDU的时间。当中断发生时，你以毫秒为单位读取系统时钟。当该TPDU得到完全处理时，你再次读取时钟。你270，000次测得0毫秒，730，000次测得1毫秒，问接收一个TPDU化多长时间？

解答：计算平均值，
（270，000×0 + 730，000×1）÷ （270，000 + 730，000）= 730，000÷1000，000 ≈0.73（毫秒）

因此，接收一个TPDU化730微妙的时间。

28．一个CPU以100 MIPS的速率执行指令。每次可以复制64比特数据，每个复制的字需花费6条指令。如果一个到达的分组需要复制两次，这个系统能处理1Gbps的线路吗？为简便起见，假定所有指令，甚至像读/写内存的指令都以100MIPS的速率执行。

解答：拷贝64比特，即8个字节要用2×6=12条指令。12条指令化120毫微妙，因此每个字节需要15毫微秒的CPU时间。 1000÷15≈66.67兆字节/秒，即系统的处理能力是66.67兆字节/秒，也就是约533Mbps，这远小于1Gbps的处理需求，所以，这个系统不能处理1Gbps的线路。

29．当老的分组仍然存在时，为了避免出现顺序号循环重复问题，可以使用64位顺序号。光纤在理论上可以用75Tbps的速率工作。试问，需要什么样的最长的分组生命周期才能确保未来的75Tbps网络在使用64位顺序号时不出现顺序号循环重复的问题？假定像TCP那样，每个字节都有自己的序号。

解答：顺序号空间的大小是2^{64}个字节，约为2×10^{19}字节， $75\div8\approx9.375$，即75Tbps的发送器每秒消耗9.375×10^{12}个序列号。$2\times10^{19}\div(9.375\times10^{12})\approx2\times10^{6}$

∴顺序号循环一周需用2×10^{6}秒。60×60×24=86400，一天有86400秒，以75Tbps速率发送，顺序号循环一周所花的时间约等于$2\times10^{6}\div86400\approx23$（天），因此，最长的分组生命周期小于3个星期可以避免顺序号循环重复问题。

30．100 MIPS 的计算机通过1千兆位的线路交换4K字节分组的数据时，分组将以超过30000个的速度到达。如果想保留一半的CPU时间去处理其它应用程序，就必须在15微秒内处理完一个分组。在15微妙的时间内，100 MIPS的计算机可以执行1500条指令。如果分组大小改成128字节（ARPANET 分组尺寸），情况会是如何？

解答：$10^{9}\div(128\times8)\approx10^{6}$， $1\div10^{6}=10^{-6}$

1微妙处理完1个分组。 考虑一半CPU时间，要求0.5微妙处理一个分组。在0.5微妙内100 MIPS的计算机可以执行50条指令。

31．对于以1Gbps速率运行的网络，是延迟（而不是带宽）成为约束因素。现在设有一个城域网（MAN），其源端机和目的端机相隔20km。问数据传输速率为多大时，由于光速导致的往返路程延迟等于1K字节分组的发送延迟？

解答：光在光纤和铜导线中的速度是大约每毫秒200公里。对于一条20公里的线路，单程延迟是100微妙，往返延迟是200微妙。1K字节就是1024×8=8192位。如果发送8192位的时间是200微妙，那么发送延迟等于传播延迟。设W是发送1位的时间，那么从等式：

$8192W=200\times10^{-6}$ 得到$W=2\times10^{-4}\div8192$， $1/W==8192\div(2\times10^{-4})\approx40\times10^{6}$，

所以，数据传输速率应为40Mbps。

32. 最小TCP MTU（最大传输单元）的总尺寸有多大？包括TCP和IP的开销，但不包括数据链路层的开销。

解答：缺省数据段大小是536字节，TCP加上20字节，IP又加上20字节，使得缺省值是总共576字节。

33．一个TCP链接使用256kbps的链路，其端到端延时为128ms。经测试发现吞吐量只有128kbps。试问窗口是多少？忽略PDU封装的协议开销以及接收方应答分组的发射时间（假定应答分组长度很小）。

解答：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256毫秒，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128毫秒。

$8X \div (256 \times 1000) = 256 \times 0.001$

$X = 256 \times 1000 \times 256 \times 0.001 \div 8 = 256 \times 32 = 8192$

所以，窗口值为8192.

34. RTP可用以发送CD质量的音频，该音频取一对16位的采样，每秒采样44 100次，每个立体声通道各采用一个采样。RTP必须每秒钟发送多少个分组？

解答：每个采样占据4个字节，考虑到发送延迟，数据段大小的缺省值是1024个字节，这样每个分组包含256个采样。立体声每秒采样44.1k次。$44100 \div 256 \approx 172$

所以RTP必须每秒钟发送172个分组。

35. 是否可以把RTP代码跟UDP代码一起放在操作系统的内核中？

解答：可以。调用方必须提供所有需要的信息，但就像UDP那样，没有理由不可以把RTP放在操作系统的内核中。

36. 假定TCP载荷是1500字节，最大分组存活时间是120秒，那么要使得TCP报文段的序列号不会循环回来而重叠，允许的最快线路速度是多大？

解答：目标是在120秒内最多发送2^{32}个字节，即每秒35，791，394个字节的载荷。TCP报文段载荷是1500字节，那么可以发送23，861个报文段。TCP开销是20个字节，IP开销是20个字节，以太网开销是26个字节。这就意味着对于1500字节的载荷，必须发送1566个字节。$1566 \times 8 \times 23，861 \approx 299Mbps$。

因此允许的最快线路速度是299Mbps；比这速度更快，就冒有在同一时间不同的TCP报文段具有相同的序列号的风险。

37. 一个CPU执行指令的速度是1 000 MIPS，数据可以一次拷贝64比特（1个字），拷贝每一个字用10条指令。如果进来的分组必须拷贝4次，那么这个系统能够处理1-Gbps的线路吗？为简便起见，假定所有的指令，即使是读或写内存的指令，都以1000-Mbps的完全速度操作。

解答：拷贝8字节（64比特）花$4 \times 10 = 40$条指令。40条指令用40毫微秒的时间。这样每

个字节需要5毫微秒的CPU时间用于拷贝。因此，该系统能够处理200M字节/秒或1600Mbps。如果不存在其它瓶颈，它能够处理1-Gbps的线路。

38.给出RPC使用UDP较之使用T/TCP的一个优点。在给出使用T/TCP的一个优点。

解答：跟使用T/TCP相比，使用UDP仅需用2个分组，而不是3个分组。然而，如果应答比较大，在1个分组中装不下，RPC就有了问题。能够解决这个问题也正是T/TCP的一个优点。

39. 在图7-9（a）中，我们看到完成RPC用了9个分组，是否有需要用10个分组的情况

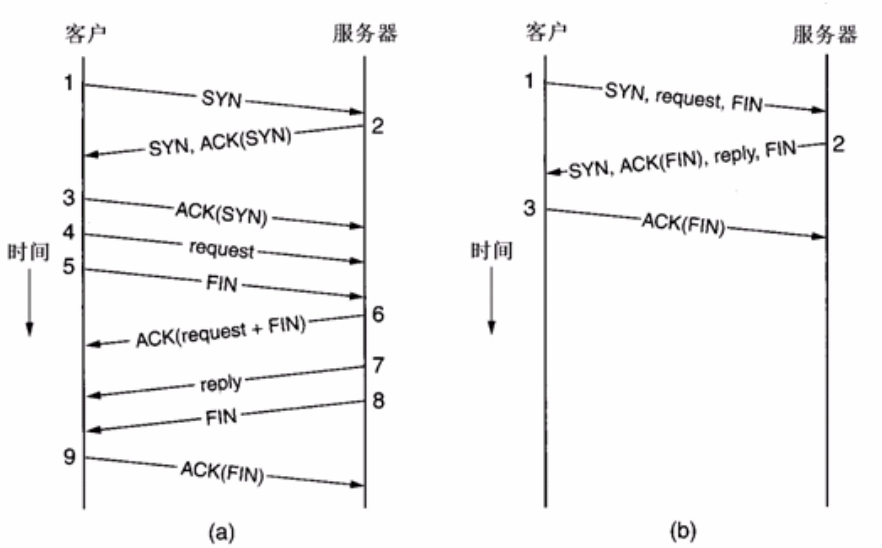


图 7-9 （a）使用常规 TCP 的 RPC （b）使用 T/TCP 的 RPC

解答：有。在图中分组6同时确认了请求和FIN。如果请求和FIN分别确认，在序列中将会有10个分组。还有，同时对回答和FIN做确认的分组9也可以分成两个单独的分组。因此，有9个分组的事实是最好的情况。

40. 我们在前面提到过，千兆位线路每秒转储80，000个分组，主机提供6250条指令处理1个分组，保留一半的CPU时间用于支持应用的处理。这个计算假定分组长度是1，500字节。试对于ARP分组尺寸128字节重新做此计算。在两种情况下都假定给出的分组大小包括了所有的开销。

解答：1500÷128≈11.72，分组缩小到原来的1/11.72，所以每秒钟得到的分组数目增加到11.72倍，因此，每个分组仅仅能够得到533条指令（6250/11.72≈533）。

41. 对于下列网络计算带宽-延迟乘积：

（1）T1 (1.5 Mbps)
（2）以太网（10 Mbps）
（3）T3 (45 Mbps)
（4）STS-3 （45 Mbps）

假定 RTT是100毫秒。注意，TCP头有16比特为窗口大小域预留。计算的结果有什么含义？

解答：（1）$1.5\times1000\text{kbps}\times100\times10^{-3}\div8=18.75\text{k}$字节。

（2）$10\times1000\text{kbps}\times100\times10^{-3}\div8=125\text{k}$字节。

（3）$45\times1000\text{kbps}\times100\times10^{-3}\div8=562.5\text{k}$字节。

（4）$155\times1000\text{kbps}\times100\times10^{-3}\div8=1937.5\text{k}$字节$\approx1.937\text{M}$字节。

16位的窗口尺寸意味着在必须等待确认以前发送的最多可发送64k字节（1 k字节=1024位）。这就意味着如果所使用的网络技术是以太网、T3或STS-3，发送方不能够连续传输并保持管道充满。

42. 在一个对地静止的卫星上的50-Mbps的通道的带宽-延迟乘积是多少？如果分组长度是1500字节（包括开销），在每个分组中的窗口应该是多大？

解答：来回路程延迟大约是540毫秒，对于50-Mbps的通道

$50\times10^{6}\text{bps}\times540\times10^{-3}\div8=3{,}375{,}000$字节

$3{,}375{,}000\div1500=2250$（分组）

因此，为了充满管道，窗口应该至少2,250个分组。

43. 写出基本的运输服务原语组(运输连接建立、释放和数据传输各原语组)。试用状态转换图，画出在一个运输连接上的这些运输服务原语有效时序关系。

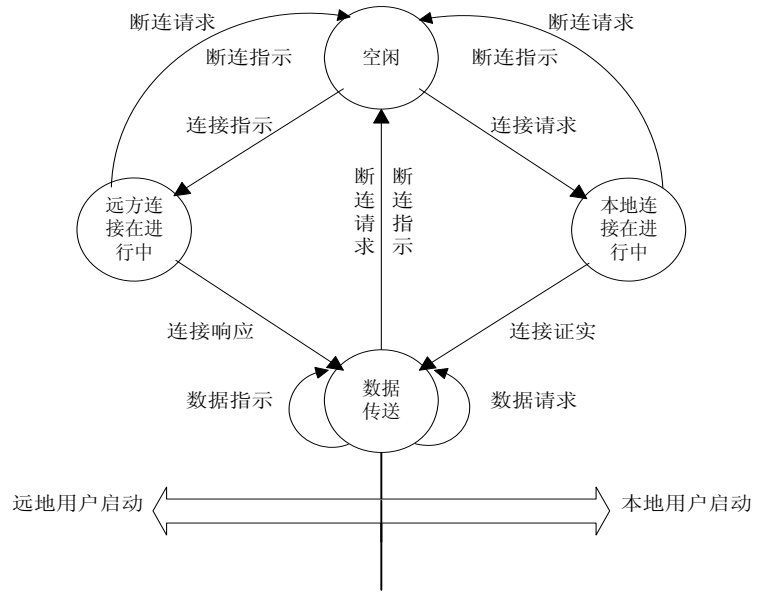
解答：

```
T_CONNECT.request,          T_CONNECT.indication,
T_CONNECT.response,         T_CONNECT.confirm,

T_DISCONNECT.request,       T_DISCONNECT.indication,

T_DATA.request,             T_DATA.indication,
T_EXPEDITED_ DATA.request,  T_EXPEDITED_ DATA.indication。
```

图7-10画出了在一个运输连接上的这些运输服务原语的有效时序关系。



注释：所有的链接都是指运输连接；数据可以是正常数据，也可以是加快数据

图 7-10　在一个运输连接上运输服务原语的有效时序关系

第 8 章　面向应用的协议和软件

本章学习重点

- OSI应用层概念
- 表示层概念
- 一号抽象语法标记
- WINDOWS NT网络和NetBIOS
- Internet中的应用层
- 文件传送协议
- 远程上机协议
- 电子邮件
- DNS
- HTTP
- 动态主机配置协议
- 多媒体
- 简单网络管理协议

8.1　基本知识点

按照国际标准化组织制定的开放系统互连参考模型，面向应用的功能包括会话层、表示层和应用层所提供的服务。会话层协议的主要目的是提供面向用户的连接服务。运输层协议负责在端点之间建立和维护连接。会话层协议通过对这种基本连接服务的增值来提供一个用户接口。表示层处理所有与数表示及传送有关的问题，包括数据转换，数据加密和数据压缩。各种计算机有它自己的表示数据的内部方法，所以需要转换和协定来保证不同的计算机可以彼此理解，这些计算机中的数据存在形式常常是复杂的数据结构，表示层的任务是把结构化的数据从发送方机器用的内部格式编码成适合于传输的比特流，然后在目的端把它解码成当地所要求的表示形式，应用层则包括应用程序。这些程序在通信中需要使用表示层为它们提供的服务。

8.1.1　OSI应用层概念

应用层提供分布式信息处理服务及用户应用进程访问这些服务的途径。OSI应用层的概念和协议又被分成几种不同的子层和应用元素。其基本概念是，应用由许多应用服务元素组成，其中有些应用服务元素完成某一方面特定的应用，它们被称为特定应用服务元素

(SASE)，例如文件传送、访问和管理(FTAM)，虚拟终端协议(VTP)和报文处理系统(MHS)。另外一些应用服务元素起通用模块的作用，它们提供各种应用共同需要的一些常用服务，诸如联系的建立和释放等等。这类应用服务元素称作公共应用服务元素(CASE)，其典型的例子有联系控制服务元素(ACSE)，可靠传送服务元素(RTSE)和远程操作服务元素(ROSE)等等。

用户的应用进程和应用层之间还有一个用户元素，它提供各种由应用层所支持的分布式信息处理服务的用户接口。典型地，它的实现形式是一套库过程或函数，被链接到需要访问所支持的分布式信息服务的用户应用进程，用户应用进程和用户元素之间的接口原语不必与特定应用实体所提供的标准服务原语相同。这样就可以使用依赖于现存厂商(因此依赖于操作系统)的用户接口原语。因此，用户元素(UE)在现实系统环境和开放系统环境之间执行必要的映射功能。

通常，应用实体支持某个范围的分布式信息处理服务。每种服务由一个特定应用服务元素提供。应用实体还包含公共应用服务元素(CASE)提供的一些一般支持服务，例如，在特定应用服务元素(SASE)执行它们特别的应用功能之前，在两个SASE之间建立一条网络范围的逻辑连接(在应用层中称作联系)。在这里还应特别指出的是，虽然为了描述的目的我们是将面向应用的3个层次(会话层，表示层和应用层)分开讨论的，但它们应该被看成是集合在一起，代表一个用户应用进程提供一种特别的应用服务的。因此，有所有3层公用的单个连接标识；也就是说，表示和会话地址是一个，而且是相同的。另外，在3个层次之间交换的服务原语的许多参数，不加改变地从一层直接映射到另一层。

8.1.2　表示层概念

对表示层的需求来自于OSI 所面向的异种计算机环境。因为不同的计算机系统用不同的方法表示信息，在可以交换信息以前，必须就某种共同的表示达成一致意见。例如，IBM系列计算机使用EBCDIC码表示字符，而大多数其它计算机使用ASCII码。为了从IBM系统传送一个字符文件到一个ASCII系统，在实际的传送期间 必须使用一种公用的表示。这种表示可以是EBCDIC、ASCII或某种其它编码。类似地，整数、浮点值和其它种类的信息，必须以多种方法在内部存储。在这些信息可以被交换之前，必须协定某种共同的格式。提供达成协定的机制正是表示层的职能。对准这一目标，表示层标准定义了多种抽象来辅助问题的解决。

当信息从一个系统传送到另一个系统时，它的表示可以改变，但它的类型和它的值必须保留。在两个应用实体可以交换任何信息之前，支持它们的表示层实体必须就如何表示被交换信息所有可能类型的值这一问题达成一致。理想情况下，每个表示实体将能够理解和表示每种可能类型的所有的值。然而，因为可能的类型是无限的，这种理想的实体是不存在的。实际情形是，用于具体通信的类型被组合成一种或多种抽象语法。

一个抽象语法可以被非正式地看成是一个命名的类型组。ISO8822给出的实际定义是“使用独立于具体表示的编码技术的标记规则描述应用层数据或应用协议控制信息”。正如这个比较正式的定义所表明的那样，一个抽象语法仅仅定义它的组成类型——它并不规定如何表示那些类型的值。在到目前为止所定义的大多数OSI抽象语法中，类型是用一种称

为1号抽象语法标记(ASN·1)的形式语言描述的。

描述应用实体所使用的类型是有用的，但仅此还不够。表示层的主要责任是决定在通信期间如何表示这些类型的值，这可以通过为每种抽象语法协商一个传送语法而得以履行。一个传送语法可以看成对某种指定的类型组(即某种抽象语法的值)进行编码的一套规则。该术语有时也描述实际的位一级表示，这种表示通过将那些规则用于特别的值而产生。对于一种可以用于一个抽象语法的传送语法，它必须能编码该抽象语法中所有类型的值。

对于一个应用实体要使用的每一个抽象语法，必须选择一个精确的传送语法，这种选择在表示连接的建立期间进行。每个协定的抽象语法/传送语法配对称为表示上下文。在两个表示层用户(即两个应用实体)之间传送的所有数据都包含在某种表示上下文内。在一条表示连接上，在任一给定时间可用的表示上下文的集合称为确定的上下文集合(DCS：Defined Context Set)。

在典情的情况下，确定的上下文集合DCS(Defined Context Set)至少包含两个表示上下文。关于抽象语法的一个非常普通的例子是由一个应用层协议所定义的PDU的集合。第2个抽象语法的例子是描述应用实体所传输的数据。在任何情况下，对于PDU和所包含的数据都需要不同的表示上下文。

在某些情况下，要精确地决定哪种表示上下文有效是不可能的。 对于这些情况可以定义一个缺省上下文。这种缺省可以在连接建立期间商定，或者也可以事前协定。 DCS（确定的上下文集合）的初始内容在表示连接的建立期间商定。然而，在某些情况下，表示用户在连接建立时可能不知道它们将需要的所有抽象语法。例如FTAM（文件传送、访问和管理）协议的两个用户必须就要传送或访问的每个文件的抽象语法问题达成一致。但是，他们可能要到文件被打开时才能知道一个文件的抽象语法，而文件打开操作只能在表示连接建立以后发生。为了允许这样的可能性，表示层提供了上下文管理。所提供的服务使表示用户可以管理DCS，即对当前的DCS进行增加和删除操作。任一方用户都可以给予表示层一个新的抽象语法，并请求表示层协定能够表示该抽象语法类型的一个传送语法。换句话说，每一方用户都可以请求建立一个新的表示上下文。类似地，任一方用户可以请求从DCS删除一个现存的表示上下文。

8.1.3 一号抽象语法标记

表示、编码、传送和解码数据结构的关键是要有一种足够灵活的并在广泛种类的应用中有用的描写数据结构的方法；它还须具有足够的标准性，使得每个人都能对它的含义具有一致的认识。作为开放系统互连研究工作的一部分，ISO推出了这样的一种方法，称为1号抽象语法标记，或简写为ASN.1，后缀“1”指这是头一个标准表示法，将来还可能出现附加标准。ASN.1标记法在国际标准8824中描述。为了传送而把ASN.1数据结构编码成位流的规则在国际标准8825中给出。

在现实生活中，有许多应用交换复杂的数据结构。每个应用都有一些与其业务有关的数据结构需要在网络上传送。这些数据结构中的某一些应用范围较广，而另一些则仅用于特别的行业或公司。

应用层包含有许多不同的应用，每个应用有许多作为APDU(应用层协议数据单元)传送

的复杂结构。这些APDU中常常有一个类型（例如布尔型或整型）段，并且在许多情况下，这些段可以被省略或赋以缺省值。因为情况比较复杂，所以我们需要用一个更加形式化的方法来描述数据结构。于是ASN.1应运而生。

ASN.1的基本思想是定义每个应用所需的全部数据结构类型（即数据类型），将其组装在一个模块或库中。当某应用要传送一个数据结构（如一个APDU）时，可将此数据结构及其ASN.1名字传给表示层。表示层根据该ASN.1的定义即可知道段的类型和长度，并知道如何将其编码，以便传送。

在连接的另一端，接收方表示层查看数据结构的ASN.1标识（在头一个或头几个字节中编码），可以知道有多少比特属于第1个字段，有多少比特属于第2个字段，以及它们的类型等。由于有这样的信息，表示层可以轻而易举地把用于传输线路上的外部格式转换为接收方计算机使用的内部格式。例如，如果所商定的整数传送格式为补码，而接收者使用反码，那么表示层可以在APDU递交给目标用户前将所有的整数转换成反码。

ASN.1不仅提供了定义类型的方法，也为这些类型提供了定义值的方法。表8-1列出了ASN.1的基本类型。这些类型用语言实现，并且成为更复杂类型的构件。这些类型的名字都是保留字，就像所有ASN.1的保留字一样总是用大写字母形式书写。

表8-1中的最后一个类型是目标标识（OBJECT IDENTIFIER）。当建立会话时，表示层要设法使双方对以下各项协商并确保达到一致：抽象语法，编码规则以及应用所使用的协议。所有这些项都是目标（实际上是库内容），并且都是由目标标识符来命名的。目标标识符通常由多个单词组成，用一个括号括起来，例如{iso standard 8571 part 4 ftam-pci(1)}就标识了一个在ISO 8571第4部分的一个目标。

表8-1　ASN.1基本类型

基本类型	含义
INTEGER	任意长的整数
BOOLEAN	TRUE或FALSE
BIT STRING	0 个或多个比特序列
OCTET STRING	0个或多个字节序列
ANY	所有类型的联合
NULL	完全没有类型
OBJECT IDENTIFIER	目标名（即一个库的内容）

上述基本类型可以通过组合来形成更复杂的类型。表8-2中列出了ASN.1用于此目的的5种构造符。第1个构造是SEQUENCE，它用来把其它类型结合在一起，构成一个类似于Pascal的记录类型。SEQUENCE（有序）的字段可以是任何类型，包括用构造符构造的类型。SEQUENCE OF 构造符用于构造单个类型的数组。 SET类型包含0个或多个组成元素的无序集合。有关的组成元素必须是可区分的。由于顺序无关紧要，所以必须包含组成元素的标识符，以保证值的表示无歧义。 SET OF类型和SEQUENCE OF类型一样，是单个类型的元素的集合。SET OF类型的元素也是无序的。当一个数据结构可以取几种不同类型之一时应使用CHOICE类型。

表8-2　ASN.1的主要构造符

构造符	含义
SEQUENCE	各种类型的有序序列
SEQUENCE OF	单个类型的有序序列，像一个数组
SET	各种类型的无序集
SET OF	单个类型的无序集
CHOICE	从一个给定序列中任取一个类型

ASN.1允许任一个数据类型或字段有一个标识自己的标签(TAG)。有4种标签，UNIVERSAL（通用，用于在ASN.1标准中定义的基本类型及某些准基本类型，如各种串类型）、APPLICATION（应用，用于OSI应用层协议）、PRIVATE（专用，用户定义他们自己的类型）以及Context Specific（上下文特有，用在需要区别字段的地方，限于一个数据类型之内）。每个标签由一个整数组成，这个整数之前是保留字UNIVERSAL、APPLICATION和PRIVATE当中的一个，或者无保留字，没有保留字即上下文特有类型的标签。标签写在方括号中，例如[APPLICATION（保留字）4（整数）]。

设置标签的目的与编码规则及传送语法密切相关。每当传送一个字段时，其类型、长度和值通常都要传送。当给类型或字段设置标签时，标签也要传送，以便标识该类型或字段。

ASN.1传送语法的目标是能在线路上以无歧义的方式表示数据结构。传送的每一个值，无论是基本类型还是构造类型，都可能由4个域组成：

① 标识符（类型或标签）；
② 数据字段按字节计算的长度；
③ 数据字段；
④ 内容结束标志（如果数据字段长度未知）。

前3个字段是必要的，最后一个字段是任选项。第1个字段起标识作用，它有如图8-1所示的3个子字段（共8位）。最高两位标识标签种类，接下来1位标明是基本类型(0)还是构造类型(1)。标签种类为00、01、10和11，分别表示UNIVERSAL、APPLICATION、上下文特有及PRIVATE。标签值在0到30之间时用剩下的5位直接编码，如果标签的值大于、等于31，则这5位为11111，真正的标签在后继的1个或多个字节中。

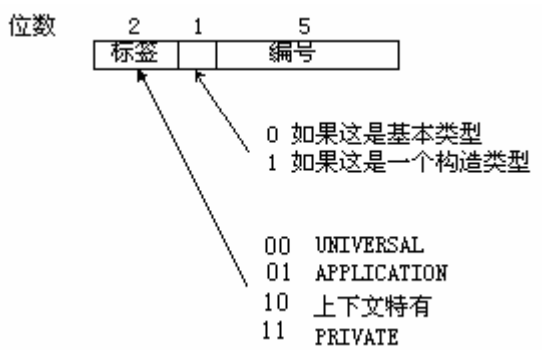


图 8-1　ASN.1 传送语法发送的数据项的首字节结构

表8-3是UNIVERSAL类型的标签编码。OBJECT DESCRIPTOR是标识目标的供人阅读的字串(OBJECT IDENTIFIER则不同，它是供机器阅读的)。EXTERNAL类型允许一个抽象语法参考另一个不同的抽象语法的一些内容，而又不必完全包括那个语法。 注意，SEQUENCE和SEQUENCE OF的UNIVERSAL类型标签相同。类似地，SET和SET OF的标签也相同。 各种各样的串(String)与不同的CCITT推荐标准有关，没有两种串使用同一个字符集的情况。最后，由于历史的原因，提供了两种不同的书写时间(Time)的方法。

表8-3　UNIVERSAL类型标签的编码

标　签	含　义	标　签	含　义
1	BOOLEAN	18	Numeric String
2	INTEGER	19	Printable String
3	BIT STRING	20	Teletex String
4	OCTET STRING	21	Videotex String
5	NULL	22	IA5 String
6	OBJECT IDENTIFIER	23	Generalized Time
7	OBJECT DESCRIPTOR	24	UTC Time
8	EXTERNAL	25	Graphic String
16	SEQUENCE 和 SEQUENCE OF	27	General String
17	SET 和 SET OF		

在传送值的标识字段的后面是长度字段，它说明数据所占的字节数。这里采用了类似于处理标签值大于30时所用的方案。也就是说，如果字节数少于128，则用1个字节直接编码；若大于128，则用两个或两个以上字节编码；其中各字节最高有效位置1，实际使用7个数据位。传送时，首先传送最高7个有效位，然后传送次高 7 个有效位。由此可见，ISO是倾向于使用“大端”顺序的（0字节作为高位字节）。

在某些情况下，数据可以用较小单元从应用层传送到表示层。如果表示层实体具有的缓冲区空间有限，则有可能在它弄清楚有多少数据之前被迫开始传输。为了处理这种情况，用一个值为128的长度码来指示数据字段是变长的。数据字段以一个特殊的内容结束标志终结。

数据字段的编码取决于数据的类型。整数以二进制补码形式编码，小于128的正整数需要1个字节，小于32768的正整数需要两个字节，如此类推。最高有效字节最先传送。布尔量FALSE编码为0，TRUE为除 0 以外任意值。布尔量编码仅占 1 个字节。

比特串（BIT STRING）的编码为其自身（不需编码）。唯一的问题是如何指示它的长度，因为长度字段说明数据所占的字节数，而不是比特数。解决的办法是在传送真正的比特串之前，先传送 1 个字节，该字节指示比特串末尾字节中未用的比特数（0—7）。这样，一个9比特串‘0 1 0 0 1 1 1 1 1’的编码为：07（未用的比特数），4F，80（十六进制），

即0000 0111 0100 1111 1000 0000。

数据字段的8比特组串（OCTET STRING）很简单，只需用标准的大端方式从左到右传送串的字节即可。空值（NULL）用一个空内容字段（字段长度为 0 ）表示。如果长度字段为 0 ，则说明所传送的是一个空值，实际上并不传送任何数值。

对于序列（SEQUENCE）和集合（SET）类型的传送，首先发送序列或集合本身的类型标识或标签，然后是其所有字段的编码总长度，最后发送字段本身。SEQUENCE的字段必须按次序发送，而SET的字段则可按任意次序发送。如果SET中有两个或多个字段的类型相同，则必须给这些字段加上标签，以便接收方能区分它们。

数据字段对于CHOICE值的编码与其实际传送的数据结构的编码相同。例如，某CHOICE在INTEGER和BOOLEAN之间取一个值，如果取值为INTEGER，则使用INTEGER的编码规则。所有字符串的编码都是 1 个字符 1 个字节，这与OCTET STRING(8 位组串)相同。

8.1.4 OSI会话层概念

会话层介于传输层和表示层之间，它利用传输层所提供的服务，并向表示层提供由它增强了的服务。会话层的主要功能是向会话用户（例如表示层实体，或者普通的用户进程）提供建立连接并在连接上有序地传送数据的一种方法。这种连接就叫做会话。会话可以用来将一个远程终端登录到远地的计算机上，或者用来传输文件；此外还有许多其它应用。

虽然会话层也有无连接原语，但是无连接的会话无法使用会话层设计的面向用户的特点。由于这个原因，我们将主要讨论面向连接的会话模型。

会话层系统提供下列服务：

- 通过在应用程序之间逻辑地连接和释放会话（也称对话）协调应用程序之间的数据交换。
- 提供同步点（也称检验点）以实现数据交换的结构化。
- 结构化用户应用的交互活动。
- 必要时为用户提供交换数据过程中的轮换规则。
- 使用同步点来保证在会话释放之前所有的数据单元都被应用程序接收。

会话与传输层的连接可以有 3 种对应关系。一种是一对一的关系。在会话层建立会话时，必须建立一个传输连接。当会话结束时，这个传输连接也就释放了。另一种是多个会话对应于一个传输连接。例如，在航空订票系统中，为一个顾客订票时在代理点终端与主计算机的订票数据库之间建立一个会话，订票结束则此会话结束。然后又有另一个顾客要求订票，于是建立另一个会话。但是，运载这些会话的传输连接没有必要不停地建立和释放。第 3 种情况是一个会话使用了多个传输连接。当传输连接在连接建立后中途失效时，这时会话层可以重新建立一个传输连接而不用废弃原有的会话。在新的传输连接建立后，原来的会话可以继续下去。这种情况通常不会发生，因为传输层自己能够从下层的失败中恢复。但是，如果传输实体是在会话实体所在的主机外部，则会话层就要承担重新恢复传输连接的责任。应该指出的是，多个会话不可以同时使用一个传输连接。在同一时刻，一

个传输连接只能对应一个会话（分时使用）。

8.1.5　WINDOWS NT网络和NetBIOS

WINDOWS NT是一个名副其实的网络操作系统。它的网络协议栈被设计成允许以多种方式进行通信，支持多种不同的协议，并且有大量的服务使用这些协议。图8-2示出了NT网络栈的设计模型。

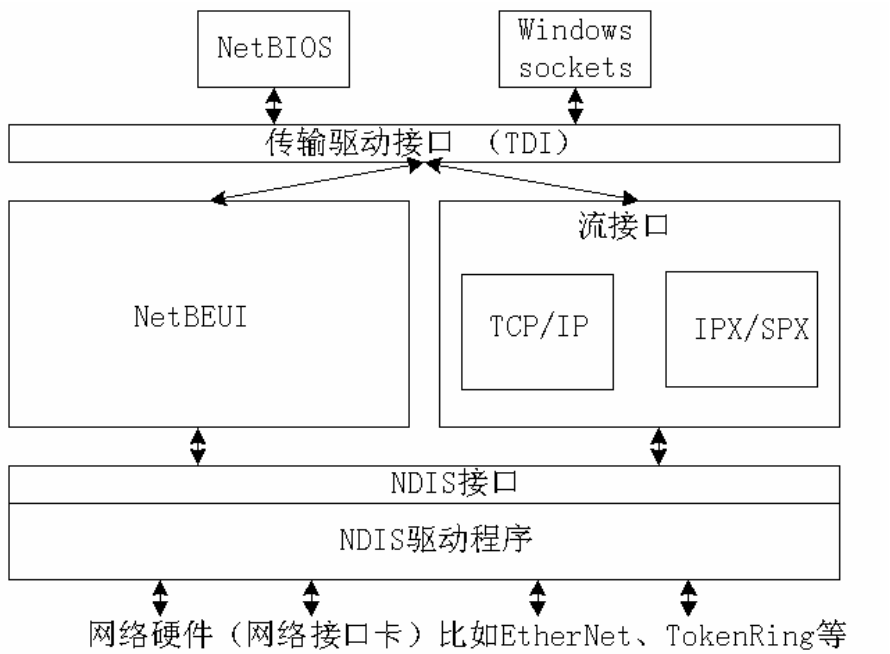


图 8-2　Windows NT 网络协议栈

Windows NT网络的结构，主要源于微软公司为OS/2所设计的LAN Manager(一种类似于NetWare的集中式的高性能的服务器，提供文件和打印机共享及其它的应用服务），尽管两者并不是完全兼容。Windows NT4.0版之前的网络结构，在某种程度上仍可视为是LAN Manager的延伸，既支持Windows NT工作站，也支持OS/2 LAN Manager工作站，共享文件数据与打印机资源。

这些兼容产品的特点，是使用了服务器消息块（SMB：Server Message Block）协议作为双方共享文件及打印资源的应用协议，一般还将这些兼容产品所构成的网络统称为微软网络（MSN：MicroSoft Network）。此外，对于Windows NT操作系统而言，网络软件已不再是操作系统的附加部分，而是其执行单元内部的成分，各种主要的网络功能，都包含在操作系统自身中。

图8-2示出的NT网络栈的最顶层由网络API（应用编程接口）组成，这些程序接口包含应用程序的实际功能函数调用。在这些网络API中最重要的可能就是Netbios（网络基本输入/输出系统）。Netbios是NT和LAN Manager网络的核心API。当一个NT系统（或其它相关系统，如Windows 95等）用微软网络（MSN）与其它系统进行通信时产生的过程调用都是

针对Netbios API而产生的。其它API也可以被应用程序调用，如Windows Sockets（或简称Winsock）提供跟Unix及其它操作系统的TCP/IP连接。

Netbios属于会话层服务的一个API，它大致地对应ISO/OSI模型中第五层（会话层）和第六层（表示层）之间的接口。它由Microsoft和IBM定义，提供一套标准的低层功能调用，应用程序可以使用它与网络上的另一节点建立通信。尽管难于编程（命名管道要容易得多），IBM的支持使Netbios成为一个广泛使用的标准。由于NT网络支持Netbios接口，所以现存的Netbios应用程序都可以不加修改地在NT网络上运行。

位于网络API下方的协议模块叫做传输驱动程序接口，或简称TDI。TDI允许网络API（如Netbios和Winsock）独立于具体的传输层协议，即使传输层协议改变了，网络API的编码仍可以不变。

在TDI的下层是传输协议本身，在NT网络上能使用三种基本协议中的任何一种：

* NetBEUI　　* TCP/IP　　* IPX/SPX

NetBEUI是一种仅用于微软网络的专用协议。它是一种快速有效的子网协议，但不具有路由功能，所以它仅适用于局域子网通信。

TCP/IP和IPX/SPX是NT网络支持的另外两个传输协议，它们都支持跨子网路由。通过TCP/IP可以实现跟UNIX系统和internet网络的通信。IPX/SPX是Novell公司开发的传输协议，包括IPX网际包交换（相当于OSI网络层）协议和SPX有序包交换传输层协议，它们都属于Xerox公司开发的XNS协议族中的子集。Windows NT利用IPX/SPX取得Netware服务器的服务，或者MSN利用它实现跨网通信。

NDIS(Network Device Interface Specification)网络设备接口规范是Microsoft和3COM公司于1989年联合制定的数据链路层接口规范，推动此规范形成的原因是解决多重传输网络协议共存于单一网络接口卡上的问题。在NDIS规范中，定义了一个标准的数据链路层接口，供上层协议栈使用，并允许上层传输网络协议跟任何低层的数据链路协议（如Ethernet，，TokenRing，，FDDI，或其它）在无需重新编码的情况下实现无缝对接。接下来在NDIS接口之下是NDIS驱动程序，是为特定的网络控制卡编写的。这些驱动程序仅需为NT编写一次，因为NDIS所提供的抽象允许同一个驱动程序连到任一更高层协议。

NDIS包括媒体访问控制层的接口规范和一个协议管理程序。一种传输协议从其跟Netbios的接口得到数据，再按照这种传输协议包装数据，然后把数据传送给由NDIS定义的接口。媒体访问控制层是OSI参考模型链路层中的一个子层，其主要部分实现为网络适配卡驱动程序，用于连接物理层和网络上层软件间的通信。协议管理程序允许多个协议被加载，并正确地链接到多个NDIS驱动程序。网络适配卡驱动程序为特定的网卡准备数据，并把数据传给网卡，网卡最后把数据位串送到网络线缆上。在相反方向，一个来自网络上的数据包通过驱动程序，送给协议管理程序模块。该模块询问每一个被安装的网络传输协议栈，以决定该数据包属于哪一种协议。假如符合安装的某一协议，那么该协议栈就接受它，否则就送给下一个协议栈。因此，NDIS是将数据包从一个协议栈到另一个协议栈地传送，直至能识别出该数据包的协议栈收到该数据包为止。

8.1.6　Internet中的应用层

一个TCP/IP网络软件既包括TCP，也包括UDP，它们提供不同的服务。大部分应用程序只使用其中的一个。如果你是一个网络系统开发人员，则可以选择能满足你要求的协议。比如说，你需要长距离电路数据传输的效率，那么选择TCP较好。但如果你需要在快速网络上实现短的等待时间，则选择UDP为宜。然而，对于某些应用，你可能难以确定使用哪一种协议为好。应用层协议可以弥补选择某一种传输层协议的不足。例如，你选择UDP，你又要求可靠性，那么应用程序的实现必须提供这种可靠性。再如，你选择了TCP，而你又需要面向记录的服务，那么应用程序必须在字节流中插入标记，作为记录的边界。

早期的TCP/IP主要用于小型机或大型机，这些机器都有自己的磁盘，是自我包含的。因此，传统的TCP/IP服务包括：

（1）文件传送

（2）远程上机

（3）电子邮件

后来使用网络的方式发生了变化，若干自我完善的大型计算机的旧模式在变迁。现在许多网络安装中都有好几种规模的计算机，包括微机、工作站、小型机和中、大型主机。虽然人们仍喜欢在一个特定的计算机上工作，但是该计算机可以调用网上的其它系统完成本地计算机不能做的工作。这种发展趋势导致了“服务器/客户”模式的网络服务。一个服务器是为网上其它系统提供某种特定服务的计算机系统，而客户则泛指使用该种服务的另一系统。

8.1.7　文件传送协议

文件传送程序使用的协议叫文件传送协议(File Transfer Protocol)，简称FTP。它允许任一台计算机的用户从另一台计算机取得文件，或传送文件到另一台计算机。

在设计一个网络文件传送协议时需要考虑的第一个问题是在这两个系统之间的协调。在发送方和接收方的管理员必须保证双方系统都在运行，发送和接收数据的应用程序也已被安装和运行。此外，如果系统在运行其它服务，或有其它网络活动在使用带宽，那么管理员必须保证有足够的资源可提供给文件传送任务。

使文件传送协议更加实用，它必须能够传送任何类型的文件。如果把传送文件的软件包括在应用代码中，那么它就是专用的了，仅允许传送特别的文件。此外，让每个应用都包括文件传送代码会使得应用程序体积大，增加了对其修改和管理的复杂度。使用协议和外部应用程序来处理文件传送就消除了这些问题。然而。文件传送协议的实现必须能够处理各种操作系统在存储文件方面的差别。在某些环境中，对于文件名可能有限制，例如在名字中允许的字符的长度。此外，不同的操作系统典型地实现不同的安全机制，通常是把它跟用户账号捆绑在一起。从一个系统启动文件传送的用户可能在接收方系统上没有一个账号，需要有一种方法，让文件匿名地传送给另一系统，而不产生对该系统的任何安全风险。文件传送软件必须能够处理这些差别，同时又不给应用的用户增加额外的负担。

根据用户和应用的需求，文件可能需要以批处理的方式传送，也可能以交互接口的方

式传送。通过使用调度程序，对于传送大的文件，在非高峰期间做批处理是方便的。交互式文件传送允许用户在需要时立即传送文件。该机制提供立即的反馈，因此用户在现场知道数据传送是否成功。对于小的文件，使用交互接口是方便的，没有必要使用批处理和调度程序。

Internet的FTP协议规范提供了上述所有必须的功能。它包括在两个不同的操作系统之间传送任何类型文件的能力。如果启动传送的用户在目的地系统上没有一个账号，那么FTP支持匿名连接和控制匿名用户的活动的能力。FTP也包括处理交互的和批处理的文件传送的能力。为了提供这些特征和功能，FTP的运行采用客户-服务器模型。接受文件服务请求的系统运行FTP服务软件，发送文件服务请求的系统运行FTP客户软件。大多数FTP在任一台机器上的实现都同时包括客户软件和服务软件。

FTP协议引入两个不同的连接。在开头的连接中，用户程序在网上发送下列一类命令：

——Log me as this user

——here is my password

——send me the file with this name

可是，一旦发出了传数据的命令，就打开第2个连接专用于传送数据。FTP协议的设计者希望允许用户在传递文件数据时继续发布命令，例如用户传输的中途发一个中止传输的命令。文件传送的安全保证通过要求用户提供对方机器的用户名和口令得以实现。FTP协议还负责处理两台机器上不同的字符集和行结束符等差异。

实际上，控制连接并不传送文件。另外，客户方也不必把每个键盘输入都发送给服务器。如果用户在FTP提示符下键入的命令不需要服务器交互，该命令就在本地解释。对于需要服务器注意的命令，FTP客户软件构建所需要的命令语法，并把信息发给FTP服务器。这一类型的信息是在客户和服务器之间的控制连接上发送的。当有一个文件要从FTP服务器传出或传送到FTP服务器时，FTP服务器要为每个文件传送建立分立的数据连接。当该文件传送结束时，数据连接被关闭。FTP控制连接依然被保持着，直到FTP服务器关闭FTP会话为止。

为了避免在控制和实际的文件传送这两种操作之间的混淆，它们每一个都被一个不同的端口号。端口号21用于FTP控制连接，端口号20用于文件传送。对控制和数据使用不同的端口和连接有许多好处。首先，该实现比较简单，FTP命令和数据之间不会互相干扰。这也允许在进行文件传送的同时用户还可以跟系统交互。例如，用户可以中止和取消文件传送。另一个好处是可以把文件的结束用作可以关闭数据连接的指示。使用这种过程意味着可以传送任意大小的文件，不必事先指定文件的大小。当到达文件的末尾（end of file）时，该文件传送完成。

8.1.8 远程上机协议

telnet允许一个用户通过TCP连接上机到网络上其它计算机，以启动一个远程会话期。从这时起，直到你退出会话之前，你在本地终端上输入的任何内容都被送往指定的远程计算机。注意，实际上你还是在跟你的计算机讲话，是telnet程序使得你的计算机不可见，尽管它一直在运行，你在本地计算机上键入的每个字符都被送往另一台计算机。

telnet是一个简单的远程终端协议，于1972年首次开发，1977年进行了更新，1984年被美国采用为军事标准。它的名字取自于TELephone NETwork，现已成为最广泛使用的协议之一。

例如，你在本地计算机终端上键入命令行“telnet delta”，则会从名叫delta的另一台计算机收到一个上机提示符，根据提示，给出你的用户名和口令，就可以在本地使用远方的delta计算机。当从delta计算机上下机时，你运行的telnet程序自动退出，你将发现，你又回到自己的计算机系统了。要提及的一点是，现在微机实现的telnet一般都包括一个对于某种通用类型终端的仿真程序(emulator)。使用telnet到另一台机器上机的过程只使用一条连接，通常是发送数据；当需要发送命令(例如置终端类型或改变某种方式)时，应使用一个特殊字符表明下一个字符是一个命令。如果用户在数据中刚好包含那个字符，那么用户计算机需要故意将该字符写两遍，表明它在这里不具有表示下一字符是命令的含义，而是将两个相同的字符（特殊字符）看成等同于一个字符的数据。

8.1.9　电子邮件

电子邮件系统的基本结构如图8-3所示, 它是一种客户机 / 服务器方式的应用。客户机软件用来处理信件，如信件的编写、阅读、管理（删除、排序等）等。服务器用来传递信件。这样的客户机软件称为UA（User Agent），而服务器软件称为MTA（Message Transfer Agent）。

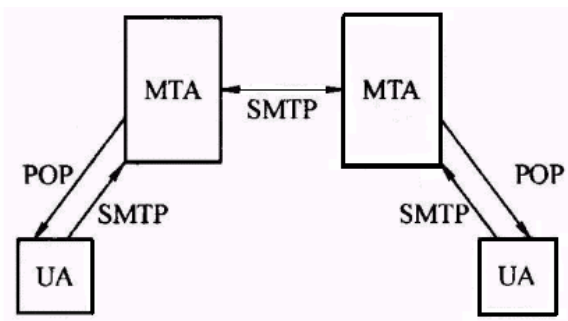


图 8-3　电子邮件系统基本结构

TCP/IP网络在 MTA之间传递邮件的协议叫SMTP(Simple Mail Transfer Protocol)。SMTP是目前使用最广泛的邮件协议，UA向MTA发送电子邮件也使用SMTP。SMTP使用的TCP端口是25，接收端在TCP的25号端口等待发送端来的Email，发送端向接收方（即服务器）发出连接要求，一旦连接成功，即进行邮件信息交换，邮件传递结束后释放连接。

下面给出的是一个典型的用SMTP传递邮件的过程。作为例子，假定一个名叫unix.ict.ac.cn的计算机（作为域ict.ac.cn的邮件服务器）要发送下列信件：

```
Date：Thur 27 June 2003 13:26:31 Beijing
From ：lu@ ict. ac. cn
To： liu @ cnc. ac. cn
Subject： meeting
```

```
Let us get together Monday at lpm
```

首先要注意的是，根据SMTP标准(RFC 822)，信件必须用纯ASCII码发送。该标准还规定了诸如邮件头、空一行、然后是信件本体这样的通用结构。详细定义的邮件头中行的语法，由关键字(keyword)及随后的具体值(value)两部分组成。在我们的例子中，收件人由liu @ cnc. ac. cn表示，它简单地对应计算机linux. cnc. ac. cn（作为域cnc.ac.cn的邮件服务器）上的用户liu； 发件人由lu @ ict. ac. cn表示，它对应计算机unix.ict.ac.cn上的用户lu。

发送方邮件软件从本地计算机的通信主机登记表(在UNIX操作系统上，主机表放在/etc/hosts文件中)或网上的名字服务器那里得知linux. cnc. ac. cn的IP地址是128. 6. 4. 2，然后邮件程序打开一条连接到128. 6. 4. 2的25号端口。unix和linux都是多用户操作系统，双方计算机的邮件服务都位于本地主机。25号是众所周知的接收邮件的端口号。一旦连接建立，发送方邮件程序就开始发送命令，下面列出的是典型的会话：

```
unix HELO ict. ac.cn
linux 250 cnc. ac. cn
unix MAIL FROM: <lu @ ict. ac. cn>
linux 250 mail accepted
unix RCPT TO: <liu @ cnc. ac. cn>
linux  250 recipient accepted
unix DATA
linux 354 start mail input; end with <CR><LF>.<CR><LF>
unix Date: Thur 27 June 2003 13:26:31 Beijing
unix From: lu @ ict. ac. cn
unix To: liu @ cnc. ac. cn
unix Subject: meeting
unix
unix Let us get together Monday at lpm ↵
unix . ↵
linux 250 OK
unix QUIT
linux 221 cnc. ac. cn service closing transmission channel.
```

每行开头都标出该行信息是从unix 还是从linux发出的。 要记住，在我们的例子中是unix主动发起连接的。按照标准，命令都使用普通正文。在示例会话中，命令HELO、MAIL、RCPT、DATA和QUIT都是标准ASCII命令，这样就给观察和诊断带来方便，可以将每个会话的轨迹放在一个记录文件中，以供检查。标准还规定，应答都以数字开头，并限定可以使用的应答格式。使用数字保证用户程序的应答无二义性。应答数字的后面辅以正文，通常只是为了供人阅读和记录，对于程序的操作没有影响。你可能已经注意到了，会话以HELO起始，它给出启动连接的发送端邮件服务器的域名，然后描述发送者和接收者，如果邮件要发给多个用户，则可以有多个RCPT命令。最后发送数据。要注意，邮件的正文用仅包含一个句点“.”的行结束。

需要强调的是，SMTP规定了对任一给定的命令可以发送的应答。以2开头的应答意味着成功，以3开头的应答表明需要有进一步的动作。4和5开头表示错误；4开头是暂时性错误，比如磁盘满；5开头则是永久性错误，例如接收用户不存在。

从上面的例子中可以看出，邮件传递分五大部分：第一部分是建立邮件连接，第二部

分是标识发送者，第三部分是标识接收者，第四部分是传递邮件数据，第五部分是结束邮件连接。

TCP/IP协议还包含了一个提供对电子邮件邮箱进行远程存取的协议。协议允许用户的邮箱安置于运行邮件服务器软件的计算机上，并允许用户从像PC这样的其它计算机上对邮箱进行存取（参见图6-9）。这个协议被称为邮局协议（POP：Post Office Protocol）。

邮局协议POP最初公布于1984年[RFC 918]。现在普遍采用的是它的第3个版本POP3[RFC 1460]，它在1993年已成为Internet的标准。和SMTP相似，在POP协议中，客户机向服务器发送命令，服务器作出响应。POP3服务器使用的端口号是110。

这样，在邮箱所在的计算机上就要运行两个服务器程序。一个是SMTP服务器程序，它用SMTP协议与邮件传输客户程序通信。另一个是POP服务器程序，它用POP协议与其它计算机上的POP客户程序通信。POP服务器只有在用户输入身份鉴别信息（如密码）后才允许其对邮箱的存取。值得注意的是，SMTP服务器接收来自发送方的信息并将它存入相应的邮箱，只能传输电子邮件，而POP服务器能够向用户提供邮箱中的信息。

在早期的TCP／IP网络中，电子邮件完全由用英文书写的正文信息组成，并且用ASCII编码表示。在这种环境中，RFC 822是一个很好的规范，它规定了邮件头格式，邮件内容则完全由用户决定。在今天的国际互联网上，这种方法已经不能够胜任所有的用户需求了。问题包括发送和接收：

- 使用不同音调的语言表示的报文（例如法文和德文）。
- 使用非拉丁字母表示的报文（例如希伯来语和俄语）。
- 使用没有字母表的语言表示的报文（例如汉语和日语）。
- 根本不包含正文的报文（例如声音和视像）。

解决这一问题的方法就是今天广泛使用的多用途Internet邮件扩展（MIME：Multipurpose Internet Mail Extension）。

MIME的基本思想是继续使用RFC 822格式，但在邮件报文体中加入结构，定义非ASCII报文的编码规则，MIME报文可以使用现有的邮件程序和协议发送。所有必须改变的就是用户使用的发送和接收程序。

MIME定义了五个新的报文头。第一个头（“MIME版本：”）只是简单地告诉接收报文的用户代理它在处理一个 MIME报文，并且告诉它所使用的 MIME版本。任何不包含“MIME版本：”头的报文都被假定是一个纯英文报文，并当作纯英文报文处理。

“内容描述：”头是ASCII字符串，说明报文中的内容。使用这个头的目的是要让接收方知道是否值得解码和阅读所收到的报文。如果该字符串是“巴巴拉的沙鼠照片”，而得到该报文的人对沙鼠不感兴趣，那么该报文很可能被丢弃，不会译码成高分辨率的彩色照片。

“内容标识：”头标识报文的内容，使用与RFC 822标准的“报文标识：”头同样的格式。

“内容传送编码：”说明如何将邮件体编码后通过网络传送，邮件网络可能拒绝除字符、数字和标点符号而外的大部分字符。

“内容类型：”最后一种头指定报文体的性质。

8.1.10 DNS

域名系统(DNS：Domain Name System)将信息跟目标相关联，它的基本功能是得到和提供因特网上关于主机(特别是IP地址)的信息。信息以查询的方式被得到，并且以回答查询的方式提供。

伯克利互联网名字域(BIND)就是 DNS的一种具体实现。BIND的主要特征包括：

（1）它是一种Internet主机名和地址查询服务，可以用以替代或补充由主机表（在UNIX操作系统中是文件/etc/hosts）提供的映射。

（2）它基于客户/服务器结构。在每个主机上都有产生查询的客户部分，在服务器系统上则有回答查询的服务器进程。

（3）它是一种分布式的名字服务，使用真正是分布式的数据库。这就意味着整个名字空间分成若干个域，而且名字与地址的映射信息分布在世界各地，世界上没有一台名字服务器具有整个因特网的全部主机信息。

（4）名字空间有一种等级式结构。因此，主机名仅需在一个域内是惟一的，而域名使得不同域内的主机名不可能混淆。

域名的解析过程如下：当某一个应用进程需要将主机名解析为IP地址时，该应用进程就成为DNS的一个客户，并将待解析的域名放在DNS请求报文中，以UDP数据报方式发给本地域名服务器。本地的域名服务器在查找域名后，将对应的IP地址放在回答报文中返回。应用进程获得目的地主机的IP地址后即可进行通信。

若本地的域名服务器不能回答该请求，则此域名服务器就暂时称为DNS的另一个客户，并向其他域名服务器发出查询请求。这种过程直到本地的域名服务器找到能够回答该请求的域名服务器为止。最终，本地的域名服务器将对应的IP地址放在回答报文中返回。应用进程获得目的地主机的IP地址后就可进行通信。

在这里需要理解名字服务器和解析器两个不同的定义。名字服务器实质上是一个程序，该程序访问一个主机数据库，回答来自其它程序的查询请求。而解析器(resolver)则与使用网络的程序装在一起，它产生送往名字服务器的查询请求，并对响应进行处理。也可以说，解析器是子程序，每个使用网络的程序都要调用它。

如果你的本地网是连到Internet，那么你的名字服务器可能与其它地方的名字服务器对话。使用名字服务器是访问其它网上Internet全部主机信息的惟一途径。

为了使用解析器，每台计算机都需要一个配置文件或类似的设施，用以指定名字查询可以送往的名字服务器的地址。你也许需要指定几个名字服务器，以备其中一个不能工作时使用其它的名字服务器，保证与外界的通信不致中断。

8.1.11 HTTP

万维网（WWW）是一个分布式的超媒体系统，它是超文本系统的扩充。一个超文本由多个信息源链接而成，并且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，而这个文档又可链接到其它的文档。这些文档可以位于世界上任何

一个接在Internet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，而超媒体文档则包含其它表示方式的信息，如图形、图像、声音、动画甚至活动视频图像。

万维网并不是一种特殊的计算机网络，而是在Internet上的一个大规模的、联机式的信息储蓄所。万维网必须解决以下几个问题：

（1）怎样标识分布在整个Internet上的万维网文档？

（2）用什么样的协议来实现万维网上各种超链的链接？

（3)怎样使不同作者创作的不同风格的万维网文档都能在Internet上的各种计算机上显示出来，同时让用户清楚地知道在什么地方存在着超链？

（4）怎样让用户能够很方便地找到所需的信息？

为了解决第一个问题，万维网使用统一资源定位符（URL）来标识万维网上的各种文档，并使每一个文档在整个Internet的范围内具有惟一的标识符。为了解决上述的第二个问题，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。为了解决上述的第三个问题，万维网使用超文本标记语言（HTML），使得万维网页面设计人员可以很方便地用一个超链从一个页面的某处链接到Internet上的其它任何一个万维网页面，并且能够在自己的计算机屏幕上将这些页面显示出来。最后，用户可使用各种各样的WWW信息搜索工具。

HTTP是传送信息的协议，相关的信息传送是为了能够高效率地完成超文本链接所必须的。从层次的角度看，HTTP是面向事务的（transaction-oriented）应用层协议，它是万维网上能够可靠地交换文件（包括文本、声音、图像等各种多媒体文件）的重要基础。

每个万维网网点都有一个服务器进程，它不断地监听TCP的端口 80，以便发现是否有浏览器（即客户进程）向它发出连接建立请求。一旦监听到连接建立请求并建立了TCP连接之后，浏览器就向服务器发出浏览某个页面的请求，服务器接着就返回所请求的页面作为响应。最后，TCP连接就被释放了。在浏览器和服务器之间的请求和响应的交互，必须按照规定的格式并遵循一定的规则。这些格式和规则就是HTTP。

HTTP规定在HTTP客户与HTTP服务器之间的每次交互都由一个ASCII码串构成的请求和一个“类MIME（即「RFC 822」MIME-like）”的响应组成。虽然大家都使用TCP连接进行传送，但标准并没有这样明确规定。

虽然HTTP使用了TCP，但HTTP协议是无状态的（stateless）。也就是说，每一个事务都是独立地进行处理。当一个个事务开始时，就在万维网客户与万维网服务器之间产生一个TCP连接，而当事务结束时就释放这个TCP连接。HTTP的无状态特性很适合它的典型应用。用户在使用万维网时，往往要读取一系列的网页，而这些网页又可能分布在许多相距很远的服务器上。将HTTP协议做成无状态的，可使读取网页信息完成得较迅速。HTTP协议本身也是无连接的，虽然它使用了面向连接的TCP向上提供的服务。

从HTTP的观点来看，万维网浏览器就是一个HTTP客户，而在万维网服务器等待HTTP请求的进程常称为HTTP daemon，有的文献将它缩写为HTTPD。HTTP daemon在收到HTTP客户的请求后，经过一些必要的处理，将所需的文件返回给HTTP客户。

HTTP规格说明定义了三种不同的操作：直接TCP连接，多段TCP连接，以及通过高速缓存的操作。

简单的情况就是用户代理与起点服务器直接建立了一个TCP连接。用户代理就是在一个端用户的计算机上运行的万维网浏览器程序。起点服务器就是用户想获取的资源所驻留的服务器。客户先发起TCP连接。在和服务器建立了TCP连接后就发送HTTP请求。这个请求包括一个特定的命令（指出使用什么方法），一个URL，和一个“类MIME”报文，它包括一些请求参数、客户的信息，或一些附加的内容信息。

当服务器收到请求后，就试图完成所请求的动作，接着就返回HTTP响应。响应包括状态信息，成功或出错代码，一个类MIME报文，包括有关服务器的信息、有关响应自身的信息，或其他的一些信息。接着就释放TCP连接。

第2种操作在用户代理与起点服务器之间没有直接的TCP连接。相反，在用户代理与起点服务器之间有多段TCP连接，这些连接经过一个或多个中间系统。每一个中间系统起着中继的作用：将请求传送到服务器，再将响应传送到客户。

第3种操作通过高速缓存，高速缓存将以前的一些请求和响应都暂存起来。当与暂存的请求一样的新的请求到达时，高速缓存就将暂存的响应发送出去，而不需要按URL的地址直接去访问该资源。高速缓存可在客户或服务器端工作，也可在中间系统上工作。

8.1.12 动态主机配置协议

在IP网络上的每个设备都需要有一个具唯一性的主机号，才能够正确地进行通信。对于大的或可能经常改变的网络，手工地给每个机器分配号码可能是一项繁琐的工作。动态主机配置协议（DHCP）提供了一个动态地给系统分配IP号码和其它IP信息的选择。在具有移动系统的环境中，像是膝上机和笔记本这样的设备经常在不同的网络中移动，使用一种服务来分配IP地址更为可取。DHCP还提供给诸如服务器这样的特别的系统分配永久号码的功能，因此当系统重新引导时，IP号码仍然保持不变。

DHCP的工作采用客户-服务器模型，还没有一个IP地址的系统向DHCP服务器请求地址。这一过程典型地是在系统引导的时候执行，从而使得它可以得到一个IP地址，访问网络和其它资源。由于系统在它启动时没有IP地址，它必须发送一个DHCP发现（DHCPDISCOVER）报文寻找DHCP服务器。这个DHCPDISCOVER报文使用特殊的IP地址255.255.255.255作为广播发送。当DHCP服务器接收到这个报文时，它对请求做应答，表示它可以提供DHCP服务。可能有多个DHCP服务器应答，请求方选择一个DHCP服务器（通常是第一个对发现报文做应答的DHCP服务器），并向它发送一个请求IP地址的报文。该DHCP服务器在它的数据库中检查，看请求方的信息（例如物理地址）是否已经被配置了一个永久的IP地址。如果没有永久的分配，DHCP就在它的可提供地址池中寻找，并启用当前尚未被使用的下一个号码。DHCP服务器把该IP地址返回给请求方，请求方就可以使用这个IP地址了。

除了IP号码和子网掩码，DHCP也可以投递其它基于IP的信息，例如，缺省网关和DNS服务器的IP地址也可以使用DHCP投递给系统。

8.1.13　多媒体

从字面上说，多媒体就是两种或两种以上的媒体。然而，大多数人所说的多媒体是指两个或两个以上连续媒体的组合，也就是，在一段已定义好的时间间隔中播放媒体，并且常常有一些与用户的交互。实际上，通常这些媒体主要就是音频和视频，即声音加上运动的图片。

8.1.13.1　音频

音频波是一维声波（压力波），当声波进入人耳时，鼓膜振动导致内耳里的微细感骨的振动，将神经冲动传向大脑。听者感觉到的这些冲动就是声音。基于相似的原理，在声波碰到麦克风后，麦克风产生出电信号，该电信号是表示声音振幅的时间函数。人耳所能听到的频率范围是20Hz—20 000Hz。

声波通过模数转换器（ADC：analog digital converter）转换为数字形式。为了将声音信号以数字比特的形式表示出来，每个△T时间对其进行一次采样。根据奈奎斯特采样定律，若声音信号中的最高频率为f，则采用2f的采样频率就足够了。由于样本的有限数字位而引入的误差叫做量化噪音。

声音采样的典型例子是电话和唱盘CD。电话系统中使用脉冲编码调制（PCM），每秒采样8000次，每次采样用7位（北美或日本）或8位（欧洲）表示。这个系统提供的数据传输速率是56kbps或64kbps。在8000次/秒的采样频率下，频率高于4kHz的信号将被丢失。唱盘CD是数字的，其采样频率为每秒44100次，足以捕获频率可高达22050Hz的信号。样本都是16位，在振幅范围内是线性的。单声道的唱盘CD需要705.6kbps的带宽，立体声则需要1.411Mbps的带宽。

8.1.13.2　视频

人类眼睛有这样一种属性，在图像出现于视网膜上后，它在消失前会滞留几毫秒。当一系列的图像以每秒50幅或更多幅的频率呈现时，眼睛将不会感觉到它所看到的不是连续的图像。所有的视频系统都是应用这一原理来产生动画。

黑白电视以一维的随时间变化的电压在屏幕上显示二维图像。摄像机扫描电子束快速地水平跨过图像并慢慢向下移动，在扫描过程中记录光的强度，在扫描到达一帧的结束处时，电子束回扫。表示成时间的函数的信号强度通过网络广播，接收器重复扫描的过程从而能够重建图像。

确切的扫描参数在国家与国家之间各不相同。北美、南美和日本使用525条扫描线，每秒30帧，长宽比为4：3。欧洲使用625条扫描线，每秒25帧，长宽比亦为4：3。虽然以25帧/秒足够提供平滑的运动效果，但在这样的帧速率下许多人，尤其是老年人，会感觉到图像的闪烁，因为在新的图像出现以前旧的图像已经消失。解决的办法是采用隔行扫描技术，首先显示所有奇数扫描线，然后显示所有偶数扫描线，而不是逐次显示所有的扫描线，每一个半帧叫做一场。实践已经证明，尽管人们会在25帧/秒的速率下觉得闪烁，但在50场/秒的速率下就不会了。

彩色视频使用的扫描方案与黑白电视相同，不同点在于显示图像时采用三束同步的电

子束代替了一束，每一束用于红绿蓝（RGB）三元色之一。这种技术的原理是基于任何颜色都是适当强度的红绿蓝三色的线性组合这一事实。然而，为了在同一信道中传输，三种颜色的信号将组合成一个组合信号。

数字系统的一个最简单的代表就是一个帧序列，每帧包含一个长方形的象素网格。一个象素是一个单个的点，代表黑或白。下一步骤就是用每个象素8比特来表示256个灰度级。这个方案能产生高质量的黑白视频。对于彩色视频，好的系统对每个RGB颜色各用8比特表示。当采用24比特/象素时，颜色数可达1600万。数字彩色图像的产生使用三个扫描束，每束用于一种颜色。为了产生平滑的运动，数字视频跟模拟视频一样，必须至少以25帧/秒的速率显示。然而，由于高质量的计算机显示器通常是以75次/秒或更高的速率显示，可根据放在内存中的图像重复扫描屏幕，所以不再需要隔行扫描，连续三次重画同一帧就足以消除闪烁现象。电影是以20帧/秒的速率播放的，每一帧被连续重画4次以去除闪烁，但运动将有些跳跃感，不连贯。

目前计算机普遍配置的便宜的显示器都是长宽比为4：3的显示器，它们可采用为电视消费市场设计的大规模生产的显象管。通常见到的配置有：640x480（VGA）、800x600（SVGA）和1024x768（XGA）。一个XGA的显示器在24比特/象素、25帧/秒时，需要472M比特/秒的传输速率。为避免闪烁，计算机存储每一帧并重画两次。

8.1.13.3 数据压缩

在现有的通信网络条件下，以非压缩的形式传送多媒体资料几乎是不可能的。唯一的希望是借助于大规模的压缩。幸运的是，在过去的几十年中大量的研究已经产生了许多压缩算法和技术，使得多媒体的传输成为可能。

所有的压缩系统都需要两个算法：一个用于压缩原文件中的数据，另一个用于在目的端解压缩还原数据，在文献中这些算法分别被称做编码和解码。通常压缩和解压缩算法是不对称的，一个多媒体文件仅被编码一次，存储到多媒体服务器上；但当它被客户观看时，可能要被解码数千次。许多实际的压缩系统竭尽全力使解码简单、迅速，即使以编码的缓慢和复杂为代价也在所不惜。不过，对于一个实时的多媒体系统，如视频会议，慢速编码也是不可接受的，编码必须瞬时完成，才能取得实时性。

视频信号在编码后又解码，结果与原始信号稍有不同一般是可以接受的。当解码的输出与原始输入并不完全相同时，系统被称为是有损的；如果输入与输出完全一致，则系统是无损的。有时候有损系统是重要的，因为少量的信息损失可能换回更大的压缩比。

压缩机制可分为两类：熵编码和信源编码。

熵编码仅处理比特流而不考虑这些比特的具体含义。它是一种通用的、无损的、完全可逆的技术，可应用于任何数据。

熵编码的典型例子是行程编码。许多数据中都会出现重复的符号（比特、数字等），它们可以用一个在该数据中不会出现的特殊标记表示，后随一个行程符号，再后随该行程符号出现的次数。如果这个特殊的标记出现在原数据中，就将它双写，就像在字符填充法中所做的那样。例如，考虑如下的十进制数字串：

3150000000000008458711111111111116354674000000000000000000000065

如果引入标记A，并使用两比特数作为重复计数，则可将上面的数字串编码为：

315A01284587A1136354674A02265

在这里，行程编码将数字串长度减少了一半。行程在多媒体中很普遍。在音频中，无声常被表示为一串零。在视频中，天空、墙壁和许多平坦表面经常出现相同颜色的行程。所有这一类的行程都能被大大压缩。

信源编码利用数据的属性进行更大程度的压缩，一般都是有损的。信源编码的典型例子是差分编码，一个值序列（如音频采样）的每个值的编码是它与前一个值的差。在相邻的两个值间的信号差别较大的情况下，所提供的表示差的字段可能不够存放差值，故差分编码是有损的。差分编码充分利用了连续数据点间不太可能出现大的跳跃这一属性。

JPEG是连续色调静止图像（如照片）的压缩标准。它对于多媒体的重要性在于，基本上可以认为运动图像的多媒体标准只是将每一帧单独用JPEG编码，加上一些帧间压缩和运动检测的附加特征。JPEG常能产生20：1甚至更高的压缩比，它基本上是对称的，编码与解码所需花费的时间基本上一样多。

MPEG 是压缩视频的主要算法，从1993年开始成为国际标准。由于电影包括图像和声音两部分，所以MPEG即可以压缩视频，也可以压缩音频。不过视频较之音频占有更高的带宽和包含更多的冗余信息。

MPEG的第一个标准是MPEG-1（国际标准11172），它的目标是产生1.2Mbps的视频录像质量的输出（NTSC的352×240）。MPEG-1能在双绞线上传输一定的距离，它也可用来将影片以CD-I或CD-Video的格式存储在CD-ROM上。

另一个标准MPEG-2（国际标准13818）开始的设计是将广播质量的视频压缩成4Mbps—6Mbps，能适用于NTSC制或PAL制广播通道。后来MPEG-2又被扩展为支持高分辨率，包括HDTV。

MPEG-4用于较低帧速（10帧/秒）和较低带宽（64Kbps）的中等分辨率视频会议，使得视频会议可在单个N-ISDN B通道上举行。本来存在MPEG-3，准备用于HDTV，但那个计划后来被取消了，并将HDTV加入到MPEG-2中。最终很可能MPEG-1在CD-ROM影片中占主导地位，MPEG-2在长距离视频传输中占主导地位。

8.1.13.4　视频点播

视频点播（VOD：video on demand）有时被比作电子录像出租店，用户从大量可供选择的录像中选择一个并拿回去观看。只有通过视频点播，这种选择才可能在家中使用电视机的远程遥控器进行，一经选择，录像立即开始播放，而免除了去商店的往返路程。

通过视频点播看电影如同其它大量潜在的新兴服务一样，只有当宽带网实现了的时候才能成为可能。图8-4是视频点播系统的一个通用模型。在这个模型中，高带宽的广域主干网处在系统的中央，与它相连的是数以千计的本地分布网络，如有线电视或电话公司的分布系统。本地分布系统到达每户人的家中，在那儿终止于机顶盒。机顶盒实际上是功能强大的特殊的个人计算机。

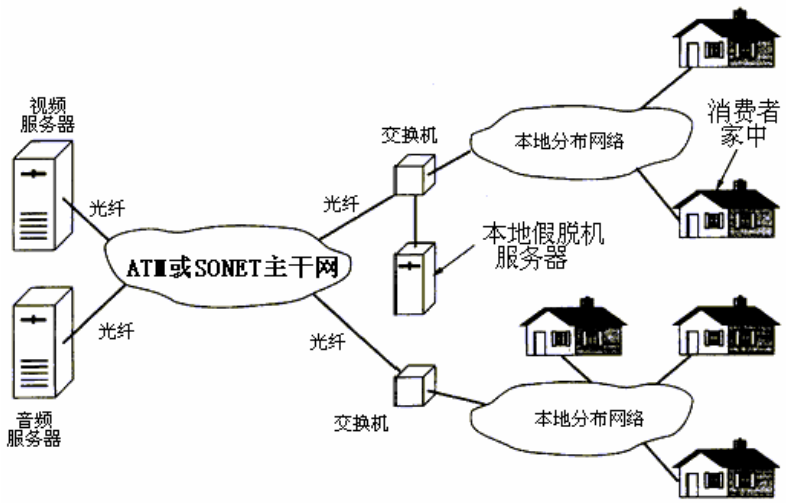


图 8-4　视频点播系统

通过高带宽的光纤连接到主干网上的有数以千计的信息提供服务器。这些服务器中有些可能提供收费电视或收费音乐，其它的服务器可能提供诸如家庭购物那样的特别服务。系统中也包括本地假脱机服务器，使视频服务提供者能被定位到更接近用户的地方，以便在高峰交通时间内节约带宽。

本地分布网络最终给每个家庭引入一个或多个MPEG流。为了解码并观看它们，需要一个网络接口、MPEG解码器和其它电子部件。这里有两种方法。在第一种方法中，人们使用他们的个人电脑解码并观看电影。要做到这一点需要购买一个特殊的插件，插件上包含几个特殊的芯片和一个与本地分布式网络接口的连接器。电影就在计算机的显示器上播放，甚至可能仅在一个窗口中。

在第二中方法中，本地网络经营者出租或卖给用户一个机顶盒，网络和电视机都连到这个盒子上。机顶盒的主要功能是与本地分布式网络接口，MPEG信号解码，同步音频和视频流，为电视机产生复合的NTSC、PAL或SECAM信号，监听、遥控和处理用户接口。附加的功能可能包括与立体声、电话和其它设备接口。

今天关于机顶盒的争论是究竟有多少功能应放置在机顶盒内和多少功能应放置在网络内，争论的最后结果还要看以后的发展。

8.1.14　简单网络管理协议

简单网络管理协议（SNMP:Simple Network Management Protocol）首先是由Internet Engineering Task Force (IETF)研究小组开发出来的。它定义了从网络设备那里收集网络管理信息的方法，还为设备指定向网络管理站报告故障和错误的途径。作为一种规范，它有三个方面的内容。

- SMI 管理信息的结构
- MIB管理信息库
- SNMP简单网络管理协议本身

网络管理站通常是运行网络管理中心软件的专用工作站。它从被管理的网络设备接收信息，通过发布SNMP命令管理SNMP设备，并且以容易理解的方式来显示网络结构和MIB信息。

因为互连网可能很庞大，而且要维护每个设备的大量信息，网络管理员需要一种组织和管理这些信息的方式。SMI提供了一种命名和组织信息的机制。MIB存储了每一个被管理对象的信息。

SMI使用一种概念树，树叶表示各种对象，用以帮助用户形象化地了解互连网络的结构。对象采用国际标准化组织提出的抽象语法标记一号（ASN．1）来表示。

如图8-5所示，树的根没有名字，有三个分枝，叫做孩子。不同的标准制定实体管理不同的分枝：ccitt（国际电报和电话咨询委员会）负责分枝0；iso(国际标准化组织)管理分枝1，ccitt和iso联合管理分枝2。

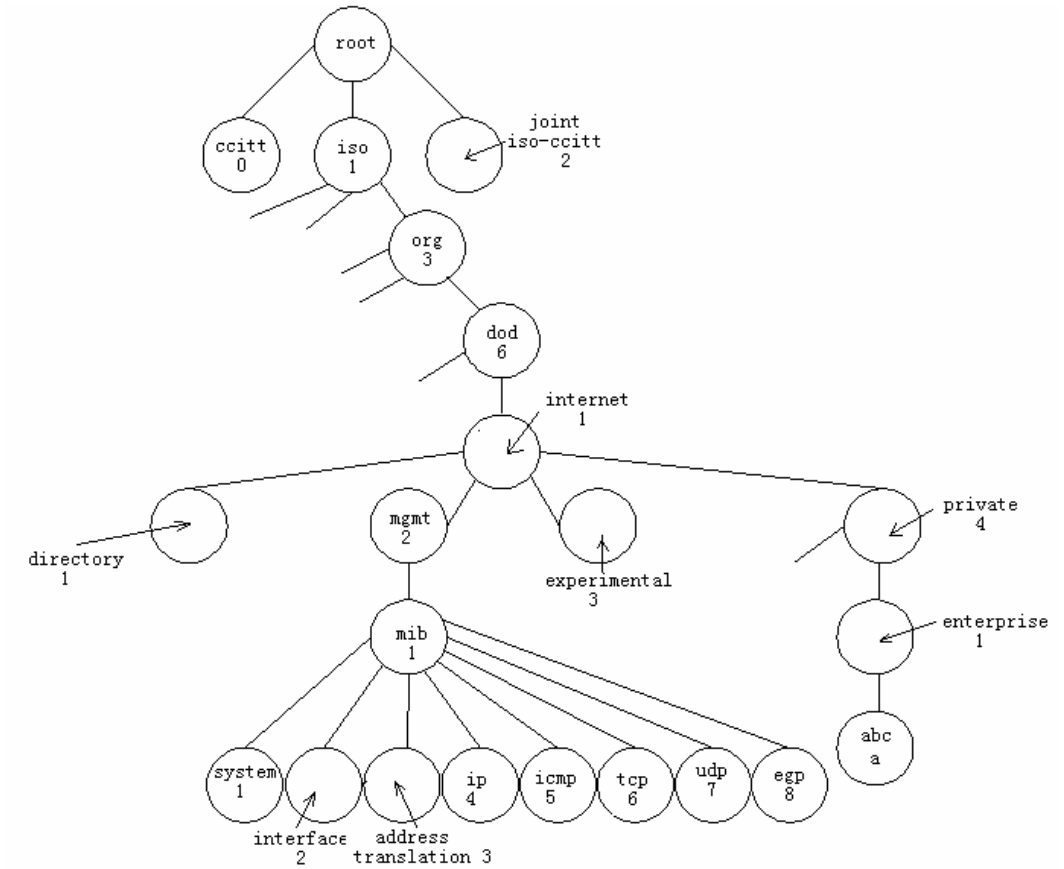


图 8-5　Internet 管理信息树

ISO将它的分枝给了几个组织，例如，它把子树3给了其它的国际组织（ org）。org将子树6给了美国国防部(dod)，dod又用子树1，表示 internet对象。这样在互联网络子树中，对象标识符以1．3．6．1开头，意思是它们属于iso 、org、dod、internet子树。 internet子树有四个分枝：directory(1), mgmt(2), experimental(3)和private(4)。

MIB定义被管理或被控制对象的信息。该管理信息库标准规定了SNMP服务器进程要维

持的一组变量，以及每个变量的语法。MIB变量记录着每个连通网络的状态、通信量统计值、发生的错误计数，还记录着内部数据结构的当前内容。例如机器的IP路由选择表。

MIB中包括一系列定义很好的已被Internet团体接受了的对象，现在有两种标准MIB版本，它们是MIB-1和MIB-Ⅱ。MIB-I标准是1988年颁布的，含有114个已经定义的对象。这些对象被划分为下列8个类别（同时参见图8-5）：

- 系统　　包含关于主机或网关操作系统的信息。
- 接口　　包含关于具体的网络接口的信息。
- 地址翻译　　包含关于地址翻译（例如ARP映射）的信息.
- ip　　包含关于IP软件的信息
- icmp　　包含关于互连网控制报文协议软件的信息.
- tcp　　包含关于传输控制协议软件的信息.
- udp　　包含关于用户数据报协议软件的信息.
- egp　　包含关于外部网关协议软件的信息.

1990年，MIB-I得到了改进，加入了更多的类别。新的版本就是MIB-II，它指出地址翻译类别已过时，并增加了类别transmission(传输)和snmp。传输类别包含关于传输介质的信息，用于接口的具体类型，例如Ethernet、Token Ring等。snmp类别包括跟snmp相关的对象，允许网络管理站管理代理的snmp部分。

虽然MIB的确切定义和MIB-II建议都相当长,但考虑它们包括的一些数据条目将有助于了解它们的内容。表8-4列出了一些MIB变量实例及它们的类别。

表8-4　MIB变量示例

MIB变量	类别	意义
sysUPTime	系统	从最后一次引导以来的时间
ifNumber	接口	网络接口的数目
ifMtu	接口	一个特别接口的最大传输单元
ipDefaultTTL	ip	IP在存活时间段中使用的值
ipInReCeives	ip	接收到的数据报的数目
ipForwDatagrams	ip	转发的数据报的数目
inOutNoRoutes	ip	路由选择失败的数目
ipReasmOks	ip	重新装配的数据报的数目
ipFragOks	ip	被分片的数据报的数目
ipRoutingTable	ip	IP路由选择表
icmpInEchos	icmp	接收到的ICMP回送请求的数目
tcpRtoMin	tcP	TCP允许的最小重传时间
tcpMaxConn	tcp	允许的最大TCP连接
tcpInSegs	tcp	TCP收到的报文段数目
udpInDatagrams	udp	收到的UDP数据报的数目
egpInMsgs	egp	收到的EGP报文的数目

列在表8-4中的大多数条目都可以存储在整数中。然而MIB也定义了更为复杂的结构。例如，MIB变量ipRoutingTable指的是一个网关的路由选择表.若干个附加变量定义路由选择表的登录项，允许网络管理协议访问每一个登录项的数据。

简单网络管理协议可以帮助网络管理人员定位并纠正TCP/IP网络中的问题。管理人员在本地计算机上调出一个SNMP客户软件，并用这个客户软件连通在远程网络设备上执行的SNMP服务器软件(也就是代理软件)。

SNMP把全部的操作都置入一种取／存模式。在概念上，SNMP仅包含两个命令，允许从一个数据项取一个值，或者把一个值存入一个数据项。所有的其它操作都定义为这个操作的衍生作用。

在SNMP使用的取／存模式中，每个服务器都维持一组概念变量，其中包括若干简单统计变量，例如已经到达的报文分组计数，也包括跟TCP/IP数据结构相对应的复杂变量，比如ARP快速缓存或IP路由选择表。SNMP报文要么要求服务器从变量中提取数值，要么把数值存入变量中；而服务器则把请求翻译成与本地数据结构相当的操作。

SNMP实际上所提供的操作比概念上要多一些，我们共有五个，其含义如下：

- get-request　　从一个具体变量取出一个值。
- get-next-request　　取一个变量的值，但不知其确切名称。
- get-response　　应答一个取操作。
- set-request　　把一个值存入一个具体的变量
- trap　　由一个事件所触发的应答。

图8-6示出了SNMP协议体系结构。它包含了我们前面讨论过的几个要素，即控制台管理程序、SNMP代理、被管理的资源（对象）和SNMP报文。SNMP报文用来在管理应用程序和SNMP被管理对象之间交换管理信息。注意，SNMP协议只规定了五种报文，即取请求、取下一个请求、取应答、置值请求和事件报文。

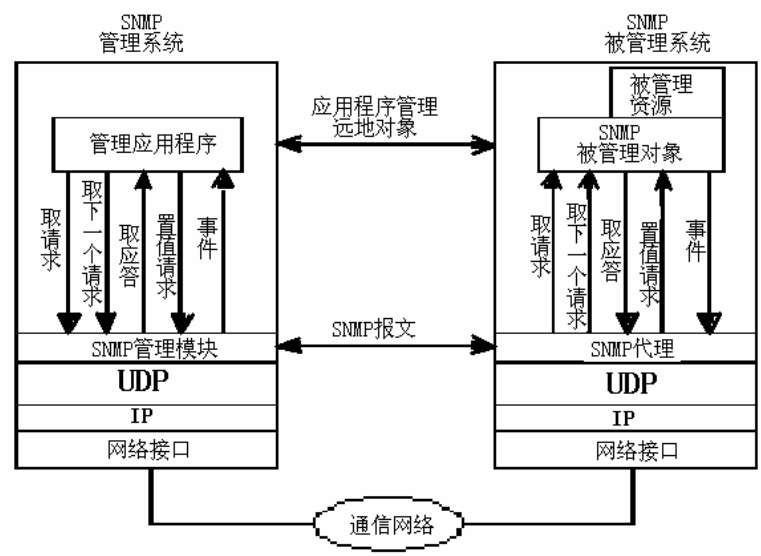


图 8-6　SNMP 协议软件的体系结构

SNMP基本上是一种轮询协议，管理程序提一个问题（询问），代理给出一个应答。UDP传输协议负责传递所有的SNMP报文,除了Trap报文使用周知端口162以外,所有其它报文都使用161号周知端口。

8.2 基本练习题

1．填空

按照国际标准化组织制定的开放系统互联参考模型，面向应用的功能包括_____层、_____层和_____层所提供的服务。

解答：按照国际标准化组织制定的开放系统互联参考模型，面向应用的功能包括__会话__层、__表示__层和__应用__层所提供的服务。

2. FTP使用哪个端口号传送数据？

a. 21　　b. 22c. 20　　d. 19

解答：c. 端口号20被用来做文件传送。端口号21被FTP用来做控制连接。

3. 下列哪一组协议属于应用层协议？

a. IP，TCP和UDP
b. ARP，IP和UDP
c. FTP，SMTP和TELNET
d. ICMP，RARP和ARP

解答：c

4. 电子邮箱有什么含义？

解答：电子邮箱通常是在服务器上一个指定的磁盘存储区域，该区域只可以被邮箱的拥有者访问。在大多数的电子邮件实现中，都把邮箱跟用户账号相关联，因此如果一个用户在一个系统上有了一个账号，他在该系统上可能也就有了一个邮箱。

5. 在一个电子邮件头中两个必须的关键字是什么？

解答：在电子邮件头内必须有一行以关键字To开头，后随一个接收者或一个接收者列表。另一行以From开头，也是必须有的，它后随邮件报文发送者的电子邮件地址。

6. 什么是邮件分发器？

解答：邮件分发器是一类程序，它把电子邮件发送给列表中的每一个接收方。

7. 填空

每个协定的抽象语法/传送语法配对称为_____。在一条表示连接上，任一

给　　定时间可用的表示上下文的集合称为_____。

解答：每个协定的抽象语法/传送语法配对称为___表示上下文___。在一条表示连接上，任一给定时间可用的表示上下文的集合称为___确定的上下文集合___。

8. SMTP是干什么用的？

解答：在发方邮件传送程序和收方邮件传送程序之间的连接是通过TCP和另一个称作SMTP（简单邮件传送协议）的协议实现的。SMTP处理邮件传送的连接建立、信息传送和连接释放。

9. 在下面列出的UNIX命令中，哪一个在远程主机上执行一条指定的命令？

a. ftp
b rcp
c. rsh
d. telnet

解答：c

10. 在下面列出的TCP/IP命令中，哪一个可以被用来远程上机到任何类型的主机？

a. ftp
b. telnet
c. rlogin
d. tftp

解答：b

11. 可以使用什么命令从FTP服务器下载文件？

解答：从FTP服务器拷贝一个文件，使用get命令；要拷贝多个文件，则使用mget命令。

12. 可以使用FTP什么命令察看你在远程FTP服务器上的当前文件目录的路径？

解答：pwd命令显示当前你的FTP会话所连接到的远程系统上的目录的路径。

13．填空

会话与传输层的连接可以有三种对应关系。一种是_____的关系。另一种是_____。第三种情况是_____。

解答：会话与传输层的连接可以有三种对应关系。一种是___一对一___的关系。另一种是___多个会话对应于一个传输连接___。第三种情况是___一个会话对应多个传输连接___。

14. 在下面列出的UNIX命令中，哪一个可以被用来远程上机到另一台UNIX主机？

a. ftp

b. telnet
c. rlogin
d. tftp

解答：c

15. 顶级域int指的是什么？

解答：顶级域int用于通过国际条例建立的国际性组织。

16. DNS MX纪录用于什么目的？

解答：MX（Mail eXchanger）用以为在电子邮件地址中的计算机名指定IP地址。

17. 一个DHCP客户在发送发现报文定位DHCP服务器时使用什么样的IP地址？

解答：使用本地广播地址 255.255.255.255。

18. 给出一个适合使用TFTP的例子。

解答：例如，无盘或没有操作系统的计算机需要找到一个BOOTP服务器下载操作系统。TFTP可以相当好地提供这种类型的文件传送服务，并且无需大量的配置工作。

19. 下列哪一项形成NFS（网络文件系统）的基础软件层次？

a. UDP
b. IP
c. RPC
d. XDR
e. 上列所有4项

解答：e

20. 为出口文件系统，你必须在下列哪个UNIX文件中指定文件系统和用户？

a. /etc/rc.local
b. /etc/fstab
c. /etc/hosts
d. /etc/exports

解答：d

21. MIME用于什么目的？

解答：MIME为在电子邮件中编码非文本数据提供指定编码机制的能力。IETF（Internet工程任务组）开发了多用途Internet邮件扩展（MIME）。MIME规范并非为编码二进制数据只定义一种技术，MIME允许发方和收方选择双方都理解且易于提供的一种编码格式。

22. 什么是HTML标签？

解答：HTML语言类似于其它的编程语言，有特别的词或短语用来指定动作和变量。HTML使用标签提供文档结构和指示动作。标签指定格式化指令或一个动作的开始，表现为一个名字被小于号和大于号围起来。为了表示一个标签的结束，在标签的名字前面使用一个小于和斜线符号（/），在标签的名字后面使用一个大于符号。

23.　给出一些可以用URL指定的协议的例子。

解答：取决于Web服务器和浏览器所支持的服务，通过URL可以使用不同的协议来访问信息。例如：

- 文件：指定在本地系统上的文件或目录。
- ftp：使用ftp发送检索信息的请求。
- http：对HTML文档的SSL(安全套接层)检索。
- mailto：用以发送邮件。
- news：访问一个运行新闻服务器的系统。
- nntp：访问一个运行新闻服务器的系统。
- telnet：用以建立一条到达目的地主机的telnet连接。

24. HTML的目的是什么？

解答：HTML（超文本标记语言）标准支配页面格式、内容规范和语法。标记语言的概念是语言本身不包括环境特有的格式化指令。取而代之的是，该语言使用重要或突出的级别来产生所希望的效果。

25. 什么是HTTP？

解答：HTTP（超文本传送协议）指定在浏览器和Web服务器之间通信的规则。

26. 填空

在TDI的下层是传输协议本身，在NT网络上能使用三种基本协议中的任何一种。这三种协议是_____、_____和_____。

解答：在TDI的下层是传输协议本身，在NT网络上能使用三种基本协议中的任何一种。这三种协议是__NetBEUI__、__TCP/IP__和__IPX/SPX__。

27. NIS（网络信息系统，也称YP）数据库放在哪种计算机上？

a. 客户机
b. 服务器
c. 服务器和客户机

解答：b

28. 填空

在TCP/IP网络中，两个应用进程之间的连接实际上是由4个数字确定的，包括双方的_____和双方的_____。

解答：在TCP/IP网络中，两个应用进程之间的连接实际上是由4个数字确定的，包括双方的__IP地址__和双方的__端口号__。

29. BIND可以被用来替代或补充下列哪一项？

a. NIS服务
b. /etc/hosts文件
c. /etc/rc.local文件

解答：b

30. 试给出术语“中间件”的定义。

解答：术语中间件用以表示一类软件开发工具，这些开发工具为开发客户-服务器类应用提供一整套过程和接口。其中，通过访问被捆扎成分立的块或对象的共享代码来开发程序的概念被称作面向对象的程序设计。

31. 定义在客户－服务器开发环境中RPC的含义。

解答：在客户－服务器开发环境中，RPC（远地过程调用）是指依赖公共共享代码库的软件开发机制。所定义的过程执行特有的小的任务，跟它们的交互通过参数控制。这些参数指定跟过程相关的细节，例如最大或最小值。当开发人员在他们的编码中使用过程时，他们使用自变量为过程所期待的参数传递值。

32. 假定你在两个不同的系统之间使用FTP传送一个声音文件，你应该为这个文件传送指定什么样的文件类型？

解答：Binary。FTP支持两种类型的文件：ASCII和Binary。ASCI选择用于传送文本文件，Binary则用于所有其它的类型。

33. 在一个子网上的客户怎样能够找到在另一个子网上的DHCP服务器？

解答：使用中继代理。为了允许DHCP服务器位于不同的子网上，路由器需要运行一个中继代理，该代理把DHCPDISCOVER分组引向DHCP服务器或可以把该分组继续向着服务器传送的下一个路由器。中继代理发送定向广播或单播报文，不把DHCPDISCOVER分组向其它子网广播。当该报文到达DHCP服务器时，服务器给请求方发回一个单播分组。

34．SNMP使用什么标准编码在管理者和代理之间传送的信息？

解答：抽象语法标记1号，即ASN.1。

35. 下列哪一组服务包括在TCP/IP软件包中？

a. 联网数据库，远程登录和文件传送
b. 远程登录，文件传送和电子邮件
c. 电子邮件，BIND和联网数据库

解答：b

36. 画出SNMP协议模型，并简述SNMP的工作过程。

解答：图9-7示出了SNMP协议体系结构。它包含控制台管理程序、SNMP代理、被管理的资源（对象）和SNMP报文。SNMP报文用来在管理应用程序和SNMP被管理对象之间交换管理信息。注意，SNMP协议只规定了五种报文，即取请求、取下一个请求、取应答、置值请求和事件报文。管理人员在本地计算机上调出一个SNMP客户软件，并用这个客户软件连通在远程网络设备上执行的SNMP服务器软件(也就是代理软件)。

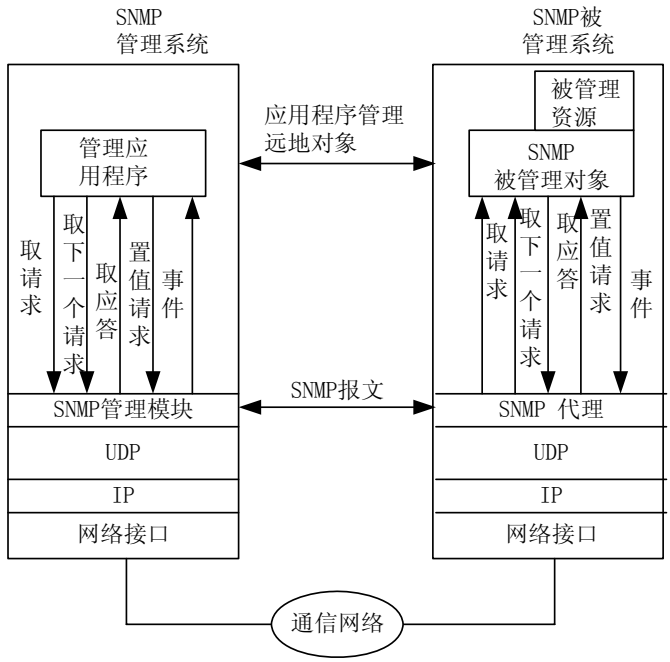


图 9-7　SNMP 协议软件的体系结构

SNMP基本上是一种轮询协议，管理程序提出一个问题（询问），代理给出一个应答。UDP传输协议负责传递所有的SNMP报文,除了Trap报文使用周知端口162以外,所有其它报文都使用161号周知端口。trap（陷阱）操作允许管理员编写服务器程序在发生一个事件时发送信息。

37. 填空题

SNMP规定了5种PDU，实际上只有两种基本操作，即

（1）读操作，用_____报文来检测被管对象的状况；
（2）写操作，用_____报文来控制被管对象的状况。

提示：get,set,trap
trap报文的用途是_____向_____报告发生的事件。
提示：管理进程、代理进程

解答：SNMP规定了5种PDU，实际上只有两种基本操作，即

（1）读操作，用_____get____报文来检测被管对象的状况；

（2）写操作，用_____set____报文来控制被管对象的状况。

提示：get,set,trap

trap报文的用途是_代理进程_____向_管理进程_报告发生的事件。

提示：管理进程、代理进程

8.3 综合应用练习题

1．下面列出的是使用TCP/IP协议通信的两台主机A和B传送邮件的对话过程，请根据这个对话回答问题？

```
A: 220 beta.gov simple mail transfer service ready
B: HELO alpha. edu
A: 250 beta.gov
B: MAIL FROM:<smith@alpha.edu>
A: 250 mail accepted
B: RCPT TO: <jones@beta.gov>
A: 250 recipient accepted
B: RCPT TO: <green@ beta.gov>
A: 550  no such user here
B: RCPT TO: <brown@ beta.gov>
A: 250 recipient accepted
B: DATA
A: 354 start mail input; end with <CR><LF>.<CR><LF>
B: Date: Thur 27 June 2003 13:26:31 BJ
B: From: smith @ alpha. edu
B: ……
B: ……
B: ……↵
B: .↵
A: 250 OK
B: QUIT
A: 221 beta.gov service closing transmission channel.
```

问题：（1）邮件发送方机器的全名是什么？发邮件的用户名是什么？

（2）发送方想把该邮件发给几个用户？他们各叫什么名字？

（3）邮件接收方机器的全名是什么？

（4）哪些用户能收到该邮件？

（5）为了接收邮件，接收方机器上等待连接的端口号是多少？

（6）传送邮件所使用的传输层协议叫什么名字？

（7）以2开头的应答意味着什么？以3开头的应答又表明什么？

（8）以4和5开头的应答各表示什么样的错误？

解答：（1）邮件发送方机器的全名是alpha. edu，发邮件的用户名smith。

（2）发送方想把该邮件发给三个用户，他们的名字分别是jones、green和brown。

（3）邮件接收方机器的全名是beta.gov。

（4）用户jones和brown能收到该邮件。

（5）为了接收邮件，接收方机器上等待连接的端口号是25

（6）传送邮件所使用的传输层协议叫TCP（传输控制协议）

（7）以2开头的应答意味着成功，以3开头的应答表明需要有进一步的动作。

（8）以4和5开头的应答表示错误，4开头是暂时性错误，比如磁盘满；5开头则是永久性错误，例如接收用户不存在。

2. 使用电子邮件网关系统（而不是存储电子邮箱的实际机器）定义电子邮件地址有什么优越性？

解答：为了使电子邮件的编址更容易，对用户更直观，分配给用户的电子邮件地址使用电子邮件的网关名，而不是邮件服务器的名字。使用不同的用户名命名风格以及使用不同的电子邮件服务器使得记住电子邮件地址比较困难。然而，如果使用电子邮件网关服务器，并使用一种账户命名标准，那么用户的电子邮件编址就可以变得比较容易。当邮件地址指向电子邮件网关时，该网关在数据库中寻找实际的邮箱地址，再把报文发送到正确的位置。例如，Blake Thurman在Texas Star公司的测试研究部门工作，他的邮箱地址是blake@testing.research.retail.texas-stars.com，Lee Ann Bliss在Texas Star公司的市场部工作，他的邮箱地址是labliss@ marketing.texas-stars.com。如果使用称作texas-stars.com的电子邮件网关服务器，上述两个雇员的邮件地址可以分别是bthurman@texas-stars.com和labliss@texas-stars.com。使用这样的地址就简便多了。

3. 许多商用计算机都有3个独特的在世界范围内具唯一性的标识符。它们是什么？

解答：它们是DNS名、IP地址和以太网地址。

4．在域cs.vu.nl的DNS数据库中有一行是

rowboat IN A 130.37.56.201

在rowboat后没有句点，为什么？

解答：它不是一个绝对名，而是相对于.cs.vu.nl.的。它实际上是rowboat.cs.vu.nl.的简写。

5. 想象在斯坦福大学计算机科学系的某个人刚写好一个新的程序，他想通过FTP发布。他把程序放在FTP目录 ftp/pub/freebies/newprog.c下。这个程序可能的URL是什么？

解答：这个程序可能的URL是ftp://www.cs.stanford.edu/ftp/pub/freebies/newprog.c

6. 有些电子邮件系统支持一个叫做“Content Return:”（内容返回：）的头段。它指定在投递不成功时是否返回消息体。这个段是属于信封还是头部？

解答：信封包含传输消息所需要的所有信息，例如目的地地址，优先级，安全级别。而头部是封装在信封内，它包含用户代理所需要的控制信息。

在本题中，“内容返回：”段属于信封，因为投递系统处理不能投递的电子邮件时需要知道它的值。

7. DNS使用UDP而不是TCP。如果一个DNS分组丢失了，没有自动恢复。这会引起问题吗？如果会，如何解决？

解答：DNS是幂等的。操作可以重复而不会有害处。当一个进程做一个DNS请求时，它启动一个定时器。如果定时器期满，它就再请求一次。这样做没有什么害处。

8. 除了可能遭受丢失，UDP分组有一个最大的长度，可以低到576字节。当查询的DNS名字超过这个长度时，将会发生什么情况？它可以用两个分组发送吗？

解答：问题不会发生。DNS名字必须比256字节短。标准要求满足这个条件。因此，所有的DNS名字都可以适配单个最小长度分组。

9. 一台具有单个DNS名字的机器可以有多个IP地址吗？这是怎样发生的？

解答：可以。IP地址由网络号和主机号两个部分构成。如果一台机器有两个以太网卡，它可以同时连到两个分开的网络上；如果是这样的话，它需要两个IP地址。

10. 一个计算机可以有两个属于不同的顶级域的DNS名字吗？如果可以，试给出一个看起来合理的例子。如果不可以，请解释原因。

解答：可以。作为例子，www.large-bank.com和www.large-bank.ny.us可以有同样的IP地址。因此，在com下面的登录项和在一个国家域下面的登录项肯定是可以的。

11. DNS服务的主要目的是什么？

解答：DNS是在IP协议集中提供的一种服务和机制，它能够把方便用户使用的设备名翻译成对应的IP地址。它的主要用途是使用户跟网络及其服务的交互变得更容易。

12. 王（wang）先生的化妆品工厂计划建立一个web网站销售他的产品。试给出该web服务器域名的一个例子，并希望该名字可以让用户容易记住。

解答：因为王先生的化妆品工厂是一个商业机构，该单位使用的顶级域是.com，他的web网站的域名的一个例子可以是www.wang-pink-dolls.com。

13. 对每个DNS服务器必须做哪3种基本配置？

解答：（1）在一个域中的DNS服务器必须知道它的每个子域的DNS服务器，例如，.texas-stars.com域的DNS服务器必须知道其子域.retail.texas-stars.com和.wholesale.texas-stars.com的DNS服务器。（2）每个DNS服务器被配置成至少知道一个根服务器的位置。事实上，大多数DNS服务器的实现都在它们的配置中提供13个DNS根服务器的完全列表。（3）每个DNS服务器至少支持一个域或子域。一个DNS服务器不可以配置成仅支持一个域或子域的一部分。然而，我们可以把一个DNS服务器配置成支持多个域或子域。

14. 近年来，具有web站点的公司的数目爆炸性增长，结果有成千上万的公司注册在com域中，引起用于这个域的顶级服务器上的重负荷。试给出在不改变命名机制的前提下消除这一问题的一个途径。在你的答案中允许要求对客户代码做必要的改变。

解答：显然有多种办法。一种办法是把该顶级服务器改变成由多台计算机组成的服务器平台（server farm）。另一种办法是设立26个分立的服务器，一个用于以a开头的名字，一个用于以b开头的名字，…等等。在采用新的服务器之后的一段时间内（比如说3年），让老的服务器继续运行，给以人们适配他们的软件的机会。

15. 一个人的电子邮件地址是“他的注册名@带有MX记录的DNS域名”。注册名可以是名、姓、首字母略写和所有其它种类的名字。假定有一个大公司发现有太多的电子邮件由于人们不知道接收者的注册名而丢失，那么是否有什么办法不用改变DNS而又能解决这个问题呢？如果回答有，试给出一个方案，并解释它是怎样工作的。如果回答没有，请说明为什么是不可能的。

解答：这是可以做的，并且比较简单。当输入邮件到达时，接收它的SMTP守护程序必须查找在报文的RCTP TO域中的注册名，系统中肯定会有一个文件或数据库，在那里可以找到这样的注册名。我们可以把这个文件扩展成具有“George.White”形式的别名，让它指向用户的邮箱。然后，电子邮件就可以使用该用户的实际名字发送。

16．一个二进制文件有3072字节长。如果用base 64编码，它将会有多长？每发送80个字节和结尾处都插入CR+LF。

解答：在 base 64编码方案中，24比特的组被分成4个6比特单位，每个单位都作为一个合法的ASCII字符发送。编码规则是A表示0，B表示1等等，接着是26个小写字母表示26到51，十个数字（0到9）表示52到61，最后，+和/分别表示62和63。=和= =分别用来指示最后一组仅包含8位或16位。回车和换行被忽略不计，因此可以任意插入它们来保持一行足够短。

在本题中，base 64编码将把报文划分成1024个单元，每个单元3字节长。每个单元被编码为4个字节，所以共有4096个字节。如果把这些字节每80字节划分为一行，将需要52行，所以需要加52个CR和52个LF。

4096+52×2=4200

综上所述，该二进制文件用 base 64编码将会有4200字节长。

17. 考虑引用的可打印MIME方案。试指出该方案中可能存在的一个问题，并提出一种解决办法。

解答：为回答本问题，首先要了解引用的可打印MIME方案。对于绝大部分都是ASCII，仅有少量非ASCII字符的报文说来，base 64编码显得有点低效。取而代之的是采用引用的可打印MIME编码，实际上就是7位的ASCII码，并且所有127以上的字符采用等号加上用2个十六进制表示的该字符的值。

总之，二进制数据要么用base 64形式发送，要么用可打印形式发送。就引用的可打印编码而论，如果一个序列以等号开始，并且后随两个十六进制数字，例如=FF，那么在正文中的这个序列将会被误解为ESC（转义）序列。解决的办法是编码等号本身，使得所有的等号都起始一个ESC序列。

18．电子邮件系统需要目录来让人们查找电子邮件地址。为了建立这样的目录，名字必须分解为标准的组成部分（例如姓和名），使得搜索成为可能。试讨论为了让一个世界性的标准被接受必须解决的问题。

解答：这个问题比人们可能想像的要复杂得多。首先，世界上差不多有一半的人先写名字后写姓；而另一半人（例如中国和日本）则刚好相反。一个命名系统必须区别任意个数的名，加上姓，而后者又可能有好几个部分，例如名字John Von Neumann就是这样。其次，有些人有中间首写字母，但没有中间名。各种称号，例如先生、小姐、夫人、女士、博士、教授或勋嚼，可以作为名字的前缀。人是有辈分的，因此必须包括Jr.（小辈）、Sr.（长辈）、III、IV等。一些人在他们的名字中使用学术称号，因此我们需要B.A.、B.Sc、M.A.、MSc、Ph.D.和其它学位。最后，有的人在他们的名字中包括某些奖励和荣誉，例如一个英格兰皇家学会的人可能在他的名字后面附加FRS（Fellow of the Royal Society）。为了让一个世界性的标准被接受就必须解决诸如此类的一系列问题。

19. 在像RFC 822这样的标准中，需要规定所允许的精确语法。即使是简单的条目也必须仔细定义。SMTP头允许在两个标记之间有空白。试给出对于在标记之间的空白的另外两种可行的定义。

解答：第一种定义是任意序列的一个或多个空格或制表键符。第二种定义是任意序列的一个或多个空格或制表键符或退格键符，要求应用所有的退格键符的最后结果至少留下一个空格或制表键符。

20. 表8-5列出了在RFC 2045中列出的MIME类型和子类型。试再说出在该表中未列出的5个MIME 类型/子类型。

表8-5　在RFC 2045中定义的MIME类型和子类型

类型	子类型	描述
Text	Plain	未格式化的文本
	Enriched	文本中含有简单的格式化命令
Image	Gif	GIF格式的静态图像
	Jpeg	JPEG格式的静态图像
Audio	Basic	声音
Video	Mpeg	MPEG格式的影视
Application	Octet-Stream	一个未解释的字节序列
	PostScript	一个以PostScript格式组织的可打印文档
Message	Rfc822	一个MIME RFC 822报文
	Partial	报文已被分割准备传输
	External-body	报文必须通过网络获取
Multipart	Mixed	按照指定顺序的各个独立部分
	Alternative	不同格式的同一报文
	Parallel	各个部分必须同时浏览
	Digest	每个部分都是一个完整的RFC 822报文

解答：一些例子和可能的帮手包括：

```
application / msexcel   (EXCEL)
application / ppt       (PowerPoint)
audio / midi            (MIDI Sound)
image / tiff            (任何图形浏览器)
video / x-dv            (QuickTime player)
```

21. POP3允许用户从一个远程邮箱获取和下载电子邮件。这是否意味着邮箱的内部格式必须标准化，使得在客户方的POP3程序可以阅读在服务器上的邮箱？请讨论你的答案。

解答：不必。POP3程序并不实际地接触远程邮箱，它发送命令给在邮件服务器上的POP3守护进程，只要该守护程序懂得邮箱格式，它就可以工作。因此，邮件服务器可以随时从一种格式改变成另一种格式，用不着通知它的客户，只要它同时改变它的POP3守护程序，使它能够懂得新的格式即可。

22. 从一个ISP的观点看问题，POP3和IMAP有一个重要的不同点。一般说来，POP3用户 每天都腾空他们的邮箱。IMAP用户则可以无限期地把他们的邮件保存在服务器上。假定你被请求忠告一个ISP应该支持哪一种协议，你会有哪些考虑？

解答：存储用户的电子邮件需要占用磁盘空间，这是要付出代价的。考虑到这一因素，使用POP3较好。在另一方面，ISP可以对超过几兆字节的磁盘存储收费，这样可以通过电子邮件服务赚钱。这一考虑又倾向于使用IMAP，因为鼓励用户把电子邮件保存在服务器上可以让他们为磁盘空间付费。

23. Webmail使用POP3还是IMAP？还是两者都不用？若回答使用二者之中的一个，请说明为什么做这样的选择。若回答两者都不用，请说明它们之中的那一个比较接近一些。

解答：两者都不用。比较而言，Webmail更接近IMAP，因为它们都允许远程检查和管理一个远程邮箱。与此相反，POP3只是把邮箱送给客户处理。

24．在发送WWW页面时，在它们的前面要加上MIME（Multipurpose Internet Mail Extensions）头，为什么？

解答：浏览器必须能够知道该页面是正文、声音、视象或其它类型，而MIME头就能提供这类信息。

25. 下面一条语句摘自一个HTML文件，

S：<H1><IMG ALIGN=MIDDLE
ALT=“W3C” SRC=“Icons/WWW/w3c_96×67.gif”>

其中ALT参数设置在〈IMG〉标签内，浏览器在什么条件下用它？怎么用？

解答：如果用户关闭了图像的自动显示，或者由于某种其它原因不能显示图像，那么在ALT中给出的正文将被显示来替代图像。

26．为一个新公司Interburger设计一个表单，使得可通过Internet预定汉堡包。该表单应

包括顾客的姓名、地址和城市，也包括对大小的选择（大或特大）以及对奶油的选择。在递交汉堡包时支付现金，故不需要信用卡信息。

解答：

```
<HTML><HEAD><TITLE>INTERBURGER</TITLE></HEAD>
<BODY>
<H1>Interburger's order form </H1>
<FORM ACTION = "http://interburger.com/cgi-bin/burgerorder"  METHOD=POST>
Name <INPUT NAME="customer" SIZE=46> <P>
Street Address <INPUT NAME="address" SIZE=40> <P>
City <INPUT NAME="city" SIZE=20> <P>
Burger size Gigantic <INPUT NAME="size" TYPE=RADIO VALUE="gigantic">
Immense <INPUT NAME="size" TYPE=RADIO VALUE="immense">
Cheese <INPUT NAME="cheese" TYPE=CHECKBOX>
<INPUT TYPE=SUBMIT VALUE="submit order"> <P>
</FORM> </BODY> </HTML>
```

27．在HTML中，怎样使一个图像成为可单击的？给出一个例子。

解答：一个超链由<A HREF= "…" >和</A>组成。在它们之间是可单击的正文。也可以把一个图像放在这里。例如：

```
<A HREF= "http://www.abc.com/foo"> <IMG SRC= "http://www.abc.com/im/im2">
</A>
```

28．给出所需的〈A〉标签，使字符串“ACM”成为http://www.acm.org的一个超链。

解答：它应该是：

```
<A HREF = "http://www.acm.org"> ACM </A>
```

29．假定WWW包含1000万个页面，平均每个页面有10个超链接。取一个页面平均花费100毫秒的时间。索引整个WWW的最短时间是多少？

解答：每个页面都要被访问。每个页面需要100毫秒，得到所有的页面要化100万秒的时间。这大约等于11.6天。跟每个页面上的链接数目是无关的，因为散列表保证每个页面仅访问一次。

30. 当用户使用Netscape点击一条链路时，会启动一个特别的帮手（helper），但当在Internet Explorer中点击同样的链路时，是否会启动一个完全不同的帮手？尽管在这两种情况下返回的MIME类型是相同的。请解释你的答案。

解答：可能。启动哪个帮手取决于在浏览器内部的配置表，对Netscape和IE可以做不同的配置。帮手应用程序通常只是接受存储内容文件的暂存文件，打开文件，显示其内容。另外，IE对待文件扩展比对待MIME类型更为严肃，文件扩展可以指示一个跟MIME类型不同的帮手。

31. 多线程的web服务器组织成如图8-7所示的结构。它花500微秒的时间接受一个请求并检查缓存。有一半的时间可以在缓存中找到文件（命中），并立即返回；另一半时间需

要对磁盘访问请求进行排队和处理，模块必须被阻塞9毫秒。为了让CPU在所有的时间都处于忙状态，假定磁盘不是一个瓶颈，那么该服务器应该有多少个模块？

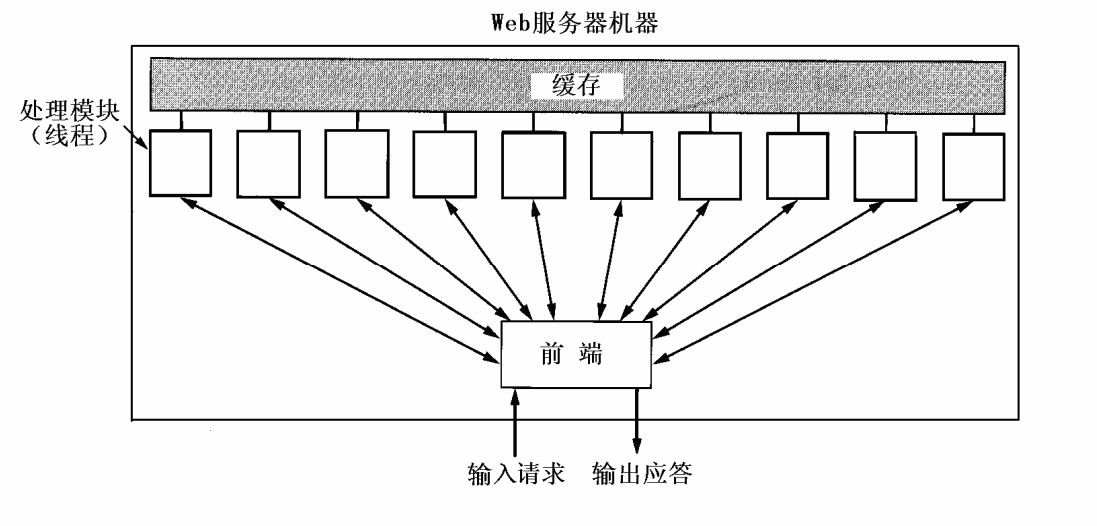


图 8-7　具有前端和多个处理模块的多线程 web 服务器

解答：如果一个模块得到两个请求，那么平均起来，有1个会在缓存中被命中，另一个在缓存中找不到。该模块所消耗的CPU总时间是500微秒×2 = 1毫秒，由于总的等待时间是9毫秒，这就给出了10%的CPU利用率。因此，有10个模块就可以保持CPU在所有的时间都处于忙状态。

32. 标准的http URL假定web服务器在端口80上倾听，然而也可以让一个web服务器在某个其它的端口上倾听。试为在一个非标准的端口上访问一个文件的URL设计一个合理的语法。

解答：RFC 1738建议做此事的方法是：
http://dns-名：端口/文件

33. URL的一种可替代的形式是使用IP地址代替它的域名。使用IP地址的一个例子是http://192.31.231.66/index.html。那么，浏览器如何知道名字是DNS名还是IP地址呢？

解答：DNS名不可以用一个数字结尾，因此不会有二义性。

34．在50Mbps的卫星信道上发布一整天的新闻（USENET新闻）需要多长时间？

解答：每天的新闻传送总量约500M字节，而且仍在不断增长。如果就按每天500M字节计算，在28.8kbps的速率下传送一天的新闻需用39小时，即使在56kbps的速率下也需要每天占用一条电话线20小时的时间。500M字节等于4000M比特，在50Mbps的卫星信道速率下，只需化4000÷50=80秒的时间就能够传完一整天新闻的交通量。

35．表8-6列出了NNTP（网络新闻传输协议）用于新闻发布的主要命令。试说明在这些命令中哪些在理论上是冗余的？

表8-6　NNTP用于新闻发布的主要命令

命令	含义
LIST	给出新闻组及文章的列表
NEWGROUPS　日期　时间	给出在指定日期/时间后创建的新闻组
GROUP grp	列出grp中的所有文章
NEWNEWS grp日期　时间	列出在指定组中在指定日期/时间后创建的的新文章
ARTICLE id	给出指定的文章
POST	我有一篇文章，我将它在此寄上
IHAVE id	我有一篇标识为id的文章，你想要吗？
QUIT	终止会话

解答：NEWGROUPS命令不是必需的，因为LIST提供了客户所要求的完全列表功能。NEWNEWS命令不是必需的，因为GROUP就能够提供在指定的组中所有文章的完全列表。客户自己可以推断哪些文章是新的。最后，POST命令不是必需的，因为IHAVE命令可以完成其功能。服务器实际上并不需要知道所提供的文章是刚投递的，或是来自一个远程节点。它可以只是核对它是否想要这篇文章。POST命令消除了检查该文章是否已经存在的必要性。

36．Java没有如C语言那样的结构或者如Pascal语言那样的记录。是否有某个其它途径能在把一组不同类的变量绑定在一起形成单个数据类型方面取得同样的效果？

解答：为了得到一个结构（struct）的效果，只须用变量定义一个类（class）但没有方法。这种类型的对象（object）然后可以用像在C语言中使用结构那样的同样方法使用。

37．图8-8示出了在一个简单的搜索引擎中使用的数据结构。试使用该数据结构列出检查一个新的URL是否已在url_table中的详细步骤。

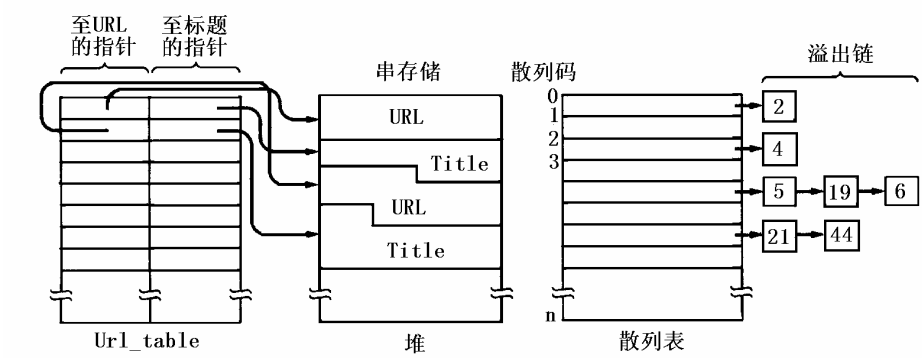


图 8-8　在一个简单的搜索引擎中使用的数据结构

解答：步骤如下：

首先，散列该URL，比如说，得到结果k。第二，从散列表的表目k起始搜查链接，找到散列值为k的一个URL序列。在url_table中依次查找这些URL中的每一个，结果找到在堆

中相应的URL串，逐个字符地把这些URL串中的每一个跟新的URL进行比较，看是否匹配。如果都不匹配，那么该URL是新的。

38. 在表8-7中，www.aportal.com保持跟踪用户的偏好，并存在一个cookie中。该机制的一个缺点是cookie被限制到4KB，因此如果偏好广泛，比如许多股票、运动队、新闻故事的类型、多个城市的天气，以及关于多个产品类别的特刊等，4KB的限制可能被打破。设计一个可替代的方法，使得能够保持跟踪偏好而又不存在这个问题。

表8-7　一些cookie示例

域	通路	内容	期满	安全
toms-casino.com	/	CustomerID=497793521	15-10-02 17:00	是
joes-store.com	/	Cart=1-00501;1-07031;2-13721	11-10-02 14:22	否
aportal.com	/	Prets=Stk:SUNW+ORCL;Spt:Jets	31-12-10 23:59	否
sneaky.com	/	UserID=3627239101	31-12-12 23:59	否

解答：只须把一个客户的ID放在cookie中，并把其偏好存储在服务器上的一个数据库中，并由客户ID对其偏好做索引。这样做，记录的大小就不受限制了。

39. Soloth银行想为它的懒于做复杂操作的客户做一个在线银行业务，使得一个客户在通过一个保密字做签名和身份验证后，银行返回一个包含客户ID的cookie。用这一方法，客户以后再访问在线银行不必标识自己或输入保密字。你认为这个想法怎么样？它姓吗？是一个好主意吗？

解答：从技术上讲，它能够工作，但却是一个可怕的主意。为得到对某个其它银行账号的访问，客户所要做的就是修改cookie。让cookie提供用户的ID是安全的，但客户应该被要求输入一个保密字来证明其身份。

40．在C和C++中没有通过语言指定整数的尺寸，而Java却这样做了。试讨论这两种方式。

解答：C语言方式允许编译器使用自然的尺寸。如果一个Java程序被移植到一个64位的CPU，整数将仍然是32位，尽管这需要硬件做额外的工作计算需要一个字的哪一半。而对于C语言，64位机器的编译器就使用64位整数。Java方式支持可移植的程序，在所有的平台上都给出同样的结果，而跟作为基础的机器无关。

41. 设计一个表单，请求用户输入两个数字。当用户点击提交（submit）按钮时，服务器返回它们的和。把服务器的程序编写成一个PHP（超文本预处理器）脚本。

解答：显示该表单的页面设计如下：

```
<html>
<head> <title> Adder </title> </head>
<body>
<form action="action.php" method="post">
<p> Please enter first number: <input type="text" name="first"> </p>
<p> Please enter second number: <input type="text" name="second"> </p>
<input type="submit">
</form>
</body>
</html>
```

做处理的PHP脚本编写如下：

```
<html>
<head> <title> Addition </title> </head>
<body>
The sum is <?PHP echo $first + $second; ?>
</body>
</html>
```

42. 对于下列每一个应用，说明

（1）它是否可能；

（2）使用PHP脚本和JavaScript，哪个更好？

（a）根据请求，显示从1752年9月以来的任意一个月的日历

解答：取决于1月1日是星期几以及某一年是否是润年，仅仅有14种年历。因此，一个JavaScript程序可以容易地包含所有的14种日历以及关于哪一年使用哪一种日历的小数据库。也可以使用一个PHP脚本，但它可能比较慢。

（b）显示从Amsterdam到New York的班机的时刻表。

解答：这需要一个大的数据库，它必须使用PHP在服务器上实现。

（c）从用户提供的系数绘制一个多项式的曲线。

解答：两者都可以使用，但JavaScript比较快。

43．一个大网由n×n机器的格栅组成，所有内部节点均有4个邻居；边上的节点有3个邻居；角上的节点有2个邻居。如果在某个机器上使用NNTP发布一篇m字节的文章，让它到达所有其它的机器要消耗多少字节的带宽？（忽略NNTP的额外开销，仅计算消息的字节）。

解答：每次报文行走一个跨段，它将到达一个新的机器。要到达所有（n^2-1）个其它机器，需要（n^2-1）个跨段，因此该报文所消耗的带宽是m（n^2-1）字节。

44．在上一道题中，如果用一个邮件列表发布消息，那么大概需要多少带宽？结果比

上一问题多了多少？

解答：在大的n×n格栅中，发送方和接收方的平均距离大约n个跨段。（n^2-1）个报文中的每一个将行走n个跨段，因此所用的带宽将是mn（n^2-1）的量级。这比使用NNTP要坏n倍。

45．什么时候需要外部观察器？浏览器怎么知道要用哪一个？

解答：如果浏览器收到具有它不能处理的MIME类型的页面，它就调用一个外部观察器来显示该页面。它可以在一个配置表中找到该观察器的名字，或者让用户选择一个。

46. 下面是一个HTML页面：

```
<html> <body>
< a href="www.info-source.com/welcome.html"> click here for info</a>
</body> </html>
```

如果用户点击该超链，会打开一条TCP连接，并有一个序列的行会被送往服务器。试列出所有被发送的行。

解答：发送的命令如下：

```
GET /welcome.html HTTP/1.1
Host:www.info-source.com
```

注意，在末尾的空行是必须有的。

47. 在一个主要的运动会的日子里，比如某个流行运动项目的冠军赛，许多人访问公认的web站点。这是一种闪发式的拥挤吗？请说明你的答案的理由。

解答：不是。在运动会的例子里，这是一个事先知道的日期，在某个web站点会有很大的拥挤，可以在各个地方建立拷贝。闪发式的拥挤在本质上则是未曾预料到的。一般说来，闪发式事件引发的拥塞是人们所不可预料的。

48. 用JavaScript编写一个程序，接受一个大于2的整数，说出它是否是一个质数。注意，JavaScript有跟C和Java同样语法的if 和while语句。模运算符是%. 如果你需要x的平方根，使用Math.sqrt（x）。

解答：显然有多个可能的答案。下面给出的是一个答案：

```
<html>
<head> <title> JavaScript test </title> </head>
<script language="javascript" type="text/javascript">

function response(test_form) {
   var n = 2;
   var has_factors = 0;
   var number = eval(test_form.number.value);
   var limit = Math.sqrt(number);
   while (n++ < limit) If (number % n == 0) has_factors = 1;
   document.open();
   document.writeln("<html> <body>");
   if (has_factors > 0) document.writeln(number, " is not a prime");
   if (has_factors == 0) document.writeln(number, " is a prime");
   document.writeln("</body> </html>");
   document.close();

}
</script>
</head>

<body>
<form name="myform">
Please enter a number: <input type="text" name="number">
<input type="button" value="compute primality" onclick="response(this.form)">
</form>
</body>
</html>
```

49. 可以使用If_Modified_Since头检查一个缓存的页面是否仍然有效。可以请求包含图像、声音、视频等内容的页面，也可以请求HTML页面。跟用于HTML相比，你认为这一技术用于JPEG图像的效果是比较好，还是比较坏？请仔细考虑效果的含义，并解释你的答案。

解答：HTML页面很有可能比JPEG文件更常被改变。多数站点经常更换HTML，但图像改变的没那么快，所以缓存访问的命中率较高。另外，图像文件通常都比HTML文件大，因此就减少延迟时间而言，图像文件使用缓存的效果更明显。

50. 让单个ISP起一个CDN（内容投递网络）的作用有意义吗？如果有意义，它是怎样工作的？如果没有意义，该想法错在哪里？

解答：有意义。该ISP联系许多个内容提供商，得到他们的许可，把他们的内容复制到该ISP的站点。内容提供商可以为此向该ISP付费。该做法的缺点是ISP联系许多个内容提供商，这个工作量很大。让一个CDN做此事就要容易一些。

51. 在什么条件下使用CDN（内容投递网络）是一个坏主意？

解答：如果内容变化很快，使用CDN不是一个好主意。例如运动会进展情况报道以及股票行情都变化很快，动态产生的页面不适合CDN。

52. 无线web终端具有低的带宽，这使得有效的编码变得很重要。设计一个方案，在无线链路上有效地把英语文本传送到一个web设备。你可以假定终端有好几兆字节的ROM和适度强大功能的CPU。

提示：考虑如何传送日文，此时每个符号都是一个单词。

解答：每个日语kanji（word）被分配一个数字，使用Unicode，总共有大约20，000个单词。对于一个英文系统，可以为65，000个常用单词分配一个16位的代码，只需传送代码。终端会在单词之间自动地加上一个空格。不在列表中的单词将使用ASCII拼写。使用这一方案，大多数的字占用2字节，比逐个传送字母要少得多。另一种方案是将8位代码用于最常使用的单词，而将比较长的代码用于不太频繁出现的单词（本征的Huffman 编码）。

53．一片光盘可容纳650MB的数据。声频CD使用压缩吗？解释你的答案的理由。

解答：声频需要1.4Mbps，即175KB/秒，在650MB的光盘上可以存储3714秒的声音，超过了1小时。光盘放音时间从不超过1个小时，因此不需要压缩，也就不使用压缩。

54．以40帧/秒传送8位/象素的非压缩VGA彩色图像的比特率是多少？

解答：$640\times480\times40\times8=98.304\times10^6$

所以比特率是98.304Mbps。

55．声波通过模数转换器（ADC）转换为数字形式。ADC以电压为输入，输出对应的二进制数。图8-9（a）是一个正弦波的例子。为了将该信号以数字的形式表示出来，每隔△t秒采样一次，如图8-9（b）所示。如果一个声波是若干正弦波的线性叠加，其中频率最高的为f，则根据奈奎斯特采样定律，采用2f的采样频率就足够了。数字采样不可能精确。如图8-9（b）所示，若3位采样只允许8个值，从–1.00到1.00，步长0.25。一个8位采样有256个不同的值。一个16位采样则有65536个不同的值。由于样本的有限数字位而引入的误差叫做量化噪音。在图8-9（c）中，由于使用4位采样表示9个信号值而产生量化噪音。在0时的第1个采样是精确的，但接着的几个采样不精确。在周期的1/32、2/32和3/32点上采样差错的百分比是多少？

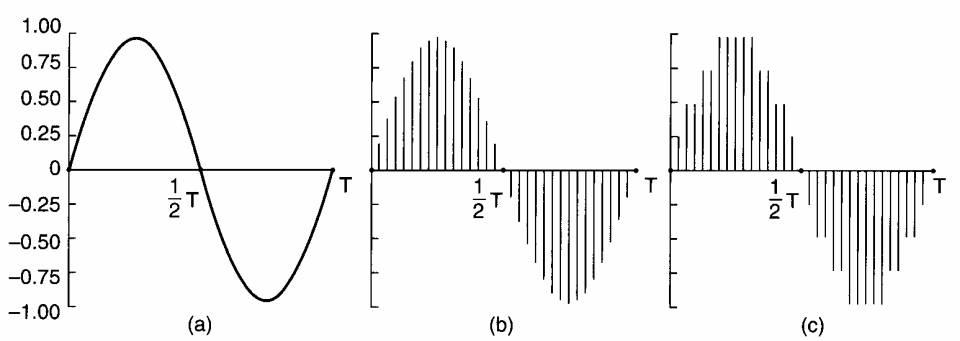


图 8-9　（a）正弦波 （b） 采样正弦波 （c）量化采样到 4 位

解答：真正的值是sin(2πi/32) ，这里的i是从1到3。在数值上，这个正弦是0.195、0.383、

和0.556。它们分别被表示成0.250、0.500和0.500。因此，差错百分比分别是28%、31%和10%.

56．MPEG帧中的一比特错误能影响除了出错帧之外的其它帧吗？请解释你的回答。

解答：能。我们知道，在MPEG中支持I帧、P帧和B帧。其中，I帧是自包含的JPEG静止图像，P帧表示与前一帧的差别，而B帧同时包含与前一帧的差别和与后一帧的差别。这样，在I帧中的一比特错误会引起在随后的P帧和B帧中的错误。事实上，该错误可能继续传播直至下一个I帧。

57．一个视频服务器有100 000个用户，假定每个用户每个月看两次电影，并且所有电影中的1/2在晚上8点至10点期间播放，在这段时间内服务器必须同时传送多少电影？如果每部电影需要4Mbps，服务器需要有多少条0C-12连接到网络？

解答：有100 000个用户，每个用户每个月看两次电影，这样，服务器每月输出200 000个影片，大约每天6600个影片。如果这些影片中的一半在晚上8点至10点期间播放，那么在这段时间内服务器必须同时传送3300个影片。如果服务器以4Mbps的速率传送每个影片，所需要的带宽将是 $4\times3300=13200$Mbps，也就是13.2Gbps。使用OC-12连接，每条连接的用户数据速率是594Mbps，

$13200\div594 \approx 23$

所以需要有23条OC-12连接。

由此看来，服务器能够同时在23条OC-12连接上服务3300个电影，可不是一个小的机器。

58．MPEG PES（打包的基本流）分组包含一个字段，给出当前传输的版权状况。该字段可能用于什么场合？

解答：不难想象未来的数字视频录像机会检查这个字段，并拒绝收录任何受版权保护的节目。国家立法甚至会要求数字视频录像机具有这一性能。

59．对于访问有10 000部电影的视频服务器，假定Zipf定律成立。如果该服务器在磁盘上存放最受欢迎的1000部电影，而剩下的9000部存放在光盘上。试给出点播磁盘上电影的分数率的表达式。

解答：Zipf定律说，当有N部电影时，对第K部最流行的电影的所有需求的分数率约为C/K，这里C = （1+1/2+1/3+ … +1/N）。在本题中，点播前r个电影的分数率是：

C/1+C/2+C/3+C/4+ … +C/r

这样，点播前1000个电影相对于点播前10 000个电影的比率将是：

（1/1+1/2+1/3+1/4+ … +1/1000）÷ （1/1+1/2+1/3+1/4+ … +1/10 000）

$\approx 7.486\div9.788\approx0.764$

因此，所有点播中的76.4%是在磁盘上的电影。

60. 可以使用一个心理声学模型来减少Internet电话所需要的带宽吗？如果可以，需要满足什么条件才能工作？如果不可以，为什么？

解答：在理论上，它是可以的，但Internet电话是实时的。对于音乐，花5分钟时间编码一个3分钟的歌不会有反对意见。但对于实时语音，那是行不通的。心理声学压缩可以用于Internet电话，但仅当有可以做具有大约1毫秒的延迟的在线即时压缩的芯片在工作时才是可行的。

61. 一个音频流服务器跟一个媒体播放器有50毫秒的单程延迟。它的输出速率是1Mbps。如果媒体播放器有1MB的缓冲区，那么你认为低端水印和高端水印的位置如何？

解答：让一个暂停命令到达服务器需要花50毫秒的时间，在这么长的时间内可以有$10^6 \times 50 \times 10^{-3} \div 8$=6250字节的数据到达。因此低水印应该高于6250×2=12，500字节（保证不会腾空），也许50，000字节是安全的。类似地，高端水印至少应是从顶部往下6250字节，但50，000字节是安全的。

62. 图8-10中示出的交织算法具有一个优点，即比较经受得住偶尔的分组丢失，在回放的过程中不会引入间隙。然而当用于Internet电话时，它有一个小的缺点。试问该缺点是什么？

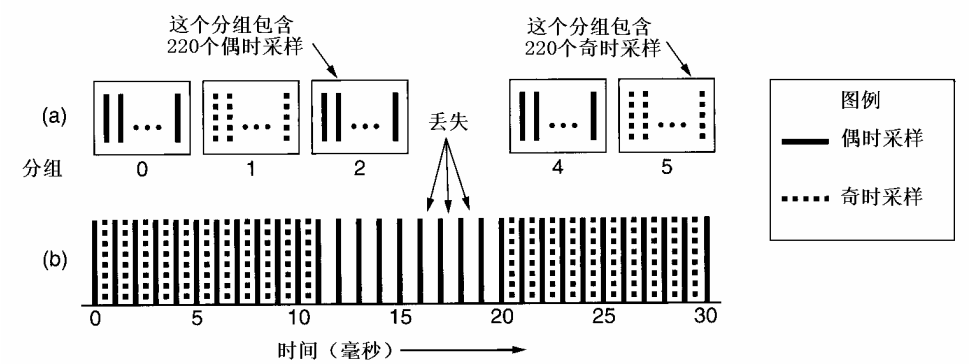


图 8-10　当分组运载交替采样时，一个分组的丢失减少暂时分辨率，而不是产生时间空隙

解答：它引入额外的延迟。在字节的方案中，在5毫秒之后就可以发送第1个分组。而在交织方案中，系统必须等待10毫秒才能发送开头5毫秒的采样。

63. 假定某人建立了一个假期守护进程，并在退出计算机系统前发出一则消息。不幸的是，接收者已经休假一周了，并且也有一个假期守护进程在运行。那么随后会发生什么样的事件？一样的回答会来回传输直到有一个人回来了吗？

解答：在退出计算机系统前发出的消息将产生一个同样的回答。它的到达又将产生同样的回答。假定每个机器记录已经应答过的电子邮件的地址，那么就不会对同一地址作更多的一样的应答。

64. 在63题中描述的假期守护进程是用户代理还是报文传送代理部分？当然它是使用用户代理建立的，但是该用户代理实际地发送回答了吗？请对你的答案加以说明。

解答：实际的回答必须由报文传送代理来做。当有一个SMTP连接到来时，报文传送代理为了应答输入的邮件，它必须检查假期守护进程是否建立，如果已经建立才发送一个回

答。用户代理部能够做这件事，因为在该用户从假期返回之前，它不会被调用。

65．猜一猜，smiley: -X (有时写成 :-#)可能的含义。

解答：它的意思是：my lips are sealed (我的嘴唇被封住了)。为保持秘密，它被用来作为对一个请求的应答。

66. 什么是MIB？

解答：可以被SNMP访问的对象称作管理信息库（MIB）。SNMP协议不定义MIB，但制定在管理者和代理之间传递的报文的格式以及在MIB中如何编码在这些报文中代表对象的变量。

67．对象tcp的对象标识符（OBJECT IDENTIFIER）是什么？

解答：对象标识符提供了一种标识对象的方法。原则上，每一个正式标准中定义的对象都能被唯一地标识。所使用的机制是定义一棵标准树，将每个标准的每个对象都放在树上的唯一的位置。根据图8-2示出的SNMP MIB的部分树，对象tcp的对象标识符是：
{1，3，6，1，2，1，6}。

68．假定必须发送一个其值为200的SNMP整数。试写出以ASN.1传送语法发送的该整数的二进制比特的表示。

解答：整数200用7个比特放不下，因此它需要14比特。表示成14比特的数字，200是00000011001000。以ASN.1传送的每个值，无论是基本类型还是构造类型，都可能由3个域组成：

标识符（类型或标签）
数字字段按字节计算的长度
数据字段

由于这里发送的第1个字节是标签，然后是长度，接着是200的值，每个字节包含7比特，第1个字节的高序位置1，因此发送的4个字节是：

00000010 00000010 10000001 01001000。

69．在ASN.1传送语法中，11比特二进制位串11100001111怎么表示？

解答：位串本身需要2个字节，加上1个字节表示最后1个字节有多少位不用（在这里是5位），再加上标签字节（位串的编码是3）和长度字节（3个字节），所以结果是下列5字节序列：

00000011 00000011 00000101 11100001 11100000

70．假定你被一个桥接器厂商雇佣，为他们的一个桥接器编写符合SNMP的代码。你读了所有的RFC，但仍有问题。你向IAB建议在某个地方给出用来描述SNMP变量的语言的一个完整的形式语法。IAB的反应是同意并指定你做这一工作。这个语法应被加入RFC 1442或RFC 1213吗？为什么？

解答：SMI（管理信息结构，RFC 1442）给出了定义数据类型的规则。MIB（管理信

息库，RFC 1213）是使用这些规则产生的实例定义。因此SMI像是程序设计语言描述，而MIB则像是以该程序设计语言编写的程序（实际上更像是C语言程序的头，而不是真正的程序）。所以所给出的形式语法应被加入RFC 1442，因为该RFC已经描述了关于ASN.1的限制条件，但尚无所允许的子集的形式语法。

71. 对于防火墙，在IP上的语音是否有跟流音频同样的问题？

解答：这取决于具体的情况。如果呼叫方不是在防火墙的后面，而且被呼方是常规的电话，那么根本没有问题。如果呼叫方在防火墙的后面，并且防火墙不介意离开场点的分组的内容，它也能工作。如果被呼方在一个不让UDP分组外出的防火墙的后面，那么它将不能够工作。

72. 发送未经压缩的800×600像素的彩色帧，每个像素8位，每秒发送40帧，其位速率有多大？

解答：位速率是800×600×40×8 = 153.6Mbps。

73．假定在服务器（名为tinker）和客户机(名为farmer)的UNIX操作系统上都已经配置了NFS，并且已向客户机出口目录/usr/share/man。试在客户机上执行命令：

安装远程目录/ usr/share/man
卸装远程目录/usr/share/man

解答：作为例子，在Digital UNIX 上可执行下列命令:

（1）安装远程目录/ usr/share/man
/usr/sbin/mount /usr/share/man@tinker /usr/tinker/man
（2）卸装远程目录/usr/share/man
/usr/sbin/umount /usr/tinker/man

第 9 章　网络安全性

本章学习重点

- 常规密钥密码体制
- 数据加密标准DES
- 公开密钥加密法
- 身份验证和数字签名
- 报文鉴别和报文摘要
- IPv6对网络安全性的支持
- 密钥分发
- 无线局域网的有线等价加密WEP
- 网络安全技术的应用

9.1　基本知识点

安全性是一个涉及面很广的话题，其中还会涉及到是否构成犯罪行为的问题。在其最简单的形式中，它主要关心的是确保无关人员不能读取、更不能修改传送给其他接收者的信息。此时，它警戒的对象是那些无权使用、但却试图获得远程服务的人。它也处理如何判断一条声称是从华龙公司来的“星期五之前付款”的报文，究竟是真的来自华龙还是来自其他单位。安全性也处理如何避免合法报文被截获和重播的问题，以及防止发送者否认曾发送过某个报文的问题。

网络安全性可以粗略地分为4个互相交织的部分：保密，身份验证，反拒认，以及完整性控制。保密是指保护信息不被未授权者访问，这是人们在谈到网络安全性时最常想到的内容。身份验证主要指在揭示敏感信息或进行事务处理之前先确认对方的身份。反拒认主要与签名有关；当一个客户下了一份1万条毛巾的订单，后来他声称每条的价格是3元，如何证明他原先答应的价格是5元呢？最后，如何确定自己收到的报文是发送者最初发出的内容，而不是被有恶意的人窜改过或伪造的呢？

所有上述问题，包括保密、身份验证、反拒认和完整性控制，也发生在传统的系统中，但却有很大的差别。保密和完整性通过使用注册过的邮品和文件锁来实现。抢劫邮车和撬开文件柜不是一件轻而易举的事。

人们能够区分常规文件的原件和复印件，但在网络上却成问题。不妨做一个测试，复印一份有效支票。星期一在银行使用支票原件，星期二尝试使用支票的复印件。注意银行里处理行为的区别。使用纸支票时，银行很容易识别是否是复制品，而使用电子支票时，

原件和复印件则无法区别。银行需要一段时间来适应这种情况。

人们通过辨认相貌、声音和笔迹来确定某个人的身份，如通过手稿上的签名、图章等来获取签字的证据。窜改行为通常能够被笔迹、纸张和墨水专家鉴定出来。这些方法在电子方式上都不可行。很明显，需要其它的解决办法。

在讨论解决方法之前，值得花些时间考虑网络安全性属于协议栈的哪一部分内容。可能没有一个单独的位置，因为安全性与每一层都有关。在物理层，可通过把传输线封装在包含高压氩气的密封管中来挫败窃听。任何钻管的尝试都会导致漏气、减压，并能触发警报装置。一些军用系统就采用了这种技术。

在数据链路层，点到点线路上的分组在离开一台机器时被编上密码，到达另一台时再解码。所有的加密细节都能在数据链路层被处理，高层对所发生的事一无所知。此方法在分组经过多个路由器时不适用，因为在每个路由器上分组都要被解码，使得它们在路由器中易受攻击。不管怎样，链路加密容易加到任何网络上，并常常被使用。

在网络层，可以安装防火墙来限制分组的进出，也可以使用 IP分组头中的安全域进行身份验证和加密处理。在运输层，整个连接都能被加密（端到瑞，即过程到过程）。尽管这些方法对保密问题有帮助，而且人们一直在努力改进，但是没有一种通用的方法能有效地解决身份认证或反拒认问题。为了解决这些问题，还必须在应用层上想办法。

9.1.1　传统加密技术

通常，人们把加密密钥与解密密钥是相同的密码体制称作常规密钥密码体制。由IBM公司研制的数据加密标准DES就属于常规密钥密码体制。按照该数据加密标准，在加密前，先对整个明文进行分组，每一组长64位。然后对每一个64位二进制数据进行加密处理，产生一组64位密文数据。最后将各组密文串接起来，即得出整个的密文。使用的密钥是64位，实际密钥长度56位，有8位用于奇偶校验。

DES算法对明文按64位分组，每组明文经初始排列（第1步）；通过子密钥k1-k16进行16次乘积变换（第2步）；再通过最终排列（第3步）得到64位密文。 k1-k16由初始密钥经过16次移位交换产生，用以对经过初始排列的64位明文做16次乘积变换。16次乘积变换的目的是使明文增大其混乱性和扩散性，使得输出不残存统计规律，使破译者不能从反向推算出密钥。

解密运算与加密运算一样，只是所取子密钥的顺序不同。加密的顺序是：

$K_1 \rightarrow K_2 \rightarrow \ldots \rightarrow K_{16}$;

解密的顺序则为：

$K_{16} \rightarrow K_{15} \rightarrow \ldots \rightarrow K_1$.

1977年1月，美国政府将该加密方法宣布为国家的数据加密标准。这个标准的确立刺激了很大一批厂商去实现加密算法的硬件化，以提高处理速度。这种密码术的核心是乘积变换，在硬件产业中常常简称为 DES（Data Encryption Standard）。这样一来，由于可以得到便宜高速的硬件，所以反过来又鼓励了许多其他用户采纳DES。

9.1.2 公开密钥加密法

所谓公开密钥密码体制就是使用不同的加密密钥与解密密钥，是一种无法由已知加密密钥推导出解密密钥的密码体制。

公开密钥密码体制的产生主要是因为两个方面的原因，一是由于常规密钥密码体制的密钥分配问题，另一个是由于对数字签名的需求。在公开密钥密码体制中，加密密钥（即公开密钥）是公开的，而解密密钥（即秘密密钥）是需要保密的。加密算法和解密算法也都是公开的。虽然秘密密钥是由公开密钥决定的，但却不能根据公开密钥计算出来。该方法最早由Diffie和Hellman（1976年）提出，并对人们研究加密系统的方式产生了根本性的变革。

在Diffie和Hellman的方法提出之前，所有的密码学家都理所当然地认为应对加密解密的密钥保密。如果人们只是根据诸如单字母表替换之类的密码来考虑问题，那么加密密钥（如果把abc变为xyz）和对应的解密密钥（把xyz变为abc）显然通常可以相互导出。Diffie和Hellman所提出的方法是使用一个加密算法E和一个解密算法D；对于所选的E和D，即使完全知道了E也不可能从其推导出D。

公开密钥加密法算法的条件与传统的加密系统完全不同，它有3个条件需要满足：

（1）D［E（P）］= P；
（2）从E导出D极其困难；
（3）使用“已知明文”的攻击方法不能破译出E。

第1个条件是说如果我们在一个加密的报文E（P）上应用D，即可得到明文。第2个条件其义自明。第3个条件之所以必要，是因为我们考虑到破译者可能会用此算法试验他想试的内容。

如果满足上述条件，就没有理由不公开E。Diffie和Hellman方法的基本思想是，任何想要接收秘密报文的个人或单位首先要设计两个算法，即E和D。这两个算法应满足上述条件。然后，公开加密算法 E（或密钥）。这也就是公开密钥加密法名称的由来。要公开密钥只需把加密算法放在一个任何人都可以读的文件中即可。

现在我们来看能否在素昧平生的A和B之间建立一个安全传输通道。假定A的加密密钥E_A和B的加密密钥E_B都放在一个公共的可读文件中（一般说来，一旦成为网络的用户，就希望他公布其加密密钥）。

A取出他的第1段报文P，计算E_B（P），然后将其发送给B。B用D_B将其解密［计算D_B［E_B（P）］= P]，没有人能读这个加密报文E_B（P），因为该加密系统被假定为足够强大，并且从已知的公开的E_B推导D_B确实很困难。

现在我们惟一要做的事就是找到符合上述所有3个条件的算法。由于公开密钥加密潜在的优越性，许多研究人员都在努力开发，并且提出了一些算法。其中一个较好的算法是由MIT（麻省理工学院）的一个研究小组（Rivest等，1978）提出来的,并被称作RSA（以其发明人Rivest、Shamir 和Adleman命名）算法。他们的方法基于数论原理。下面我们简要叙述如何使用这种方法。

（1）选择两个大素数， p和 q，均应大于 10^{100}；

（2）计算n＝p×q和z＝（p－1）×（q－1）；
（3）选择一个与z互为质数的数，令其为d；
（4）找到一个e使其满足e×d＝1 mod z。

有了这些预先计算好的参数，我们即可准备开始加密了。把明文（看作一个比特串）划分成块，使得每个明文报文p落在0≤p≤n之间。这可以通过将明文分成每块有k位的组来实现，并且 k是使得2^k＜n成立的最大整数。

加密一个报文p，需计算$c = p^e$（mod n），解密c要计算$p = c^d$（mod n）。可以证明，在指定范围内的所有p，加密函数和解密函数互为反函数。实施加密需要e和n，实施解密需要d和n。因此，公开密钥由（e，n）构成，秘密密钥由（d，n）或只是d构成。

MIT算法的安全性建立在难于对大数提取因子的基础上，如果破译者能对 n（公开的）作因子分解，那么就能找出p和q并从中得到z。如果知道了z和e，就能用Euclid的算法求得 d。值得庆幸的是，300多年来，虽然数学家们已对大数因式分解的问题作了大量研究，但并没有取得什么进展。所有已知的证据都表明：这是一个极其困难的问题。

9.1.3　身份验证和数字签名

在现实生活中，人们很注重原件和复印件的区别。例如，如果你带一张支票去银行并且能证明你的身份，那么，银行会很乐意为你兑换现金。但是，如果你带一张支票复印件到这家银行，银行职员的态度就会变得不那么友好了，因为银行对原件和复印件的区别是非常严格的。

一个相关的问题就是手迹签名。许多法律、财务以及其他文件的真实性和可靠性最终还是由授权人的亲手签名与否来确定的，复印件不算数。如果需用计算机化的报文系统代替纸墨文件的传送，就必须找出一个方法来解决上述问题。

设计一个代替手迹签名的方案是十分困难的。从根本上说，我们需要这样一个系统，一方通过该系统能以如下方式向另一方发送已签名的文件：

（1）接收方能够验证出发送方所宣称的身份；
（2）发送方以后不能否认报文是他发的；
（3）接收方不能伪造对报文的签名。

第1个条件是必须的。例如，在财务系统中，当一位顾客通过他的计算机向一家银行订购了1吨黄金时，银行需要证实发出订购要求的计算机确实属于将要付款的公司。第2个条件用于保护接收方不受欺骗。假如银行为顾客买了这吨黄金，但金价随后立即暴跌；不诚实的顾客可能会控告这家银行，宣称他从未发出任何购买黄金的订单。当银行在法庭上出示电子化订单时，该顾客可能赖帐。第3个条件是为了保护顾客的利益，防止接收方伪造对他们有利的报文签名。

在面向连接的系统中，身份验证可以在建立会话时完成。传统的方式是让用户键入一个口令来证明自己的身份。这种方法不仅将用户暴露给被动线路窃听者，同时也要求身份验证用计算机（如银行中计算机）在内部保持一个口令表，口令表本身就存在保密问题。采用公开密钥加密技术可以安全地实施身份验证，而无需保存任何口令。

当在银行开一个账户时，顾客选择一个公开密钥和一个私人密钥。把公开密钥交给银行，自己保存私人密钥。顾客请求与银行建立会话时，银行选取一个随机数，用该用户的公开密钥加密，并要求顾客将其解密后送回银行。这样，冒名顶替者就经不起这种身份验证了。另外，由于银行每次选用不同的随机数，偷录者即使录下银行和顾客间的全部来往报文也是徒劳的。

在作了初次身份验证之后，为安全起见，可能希望每一报文至少再提供一些身份验证的佐证。银行可能要求其顾客在报文中加上一条秘密口令、一个序号、传送日期和时间、以及全部明文（包括时间、日期及序号在内）的检验和。序号可以防止偷录者把报文录下后再接着发送，银行可以知道这一报文只不过是已收到报文的复制品。时间和日期可以防止偷录者把所录的报文保存下来直到该序号在下一轮中重新出现时发送。检验和可以防止偷录者伪造或修改（加密）报文。

不过，防止不诚实的顾客否认发送过报文的问题到此仍未解决。在一定的条件下，采用公开密钥加密技术有助于解决这问题。此时，加密和解密算法除了具备通常的D（E（P））= P这一特性外，还要具备E（D（P））= P特性。假设是这种情况，A可以通过传输E_B（D_A（P）来发送一个签字的明文报文到B。注意，A知道他自己的（保密的）解密密钥D_A和B的公开密钥E_B。

当B收到此报文时，他像平常那样用其私用密钥将报文转换，产生出D_A（P）。B把它存放到安全的地方，然后用E_A将其解密，从而得到最初的明文。

为了弄清签字的特征是如何实现的，我们假定A后来否认给B发送过报文P。当这个案件提交给法庭时，B可以出示P和D_A（P）。法官可以通过对D_A（P）应用E_A而很容易判明B确实收到过用D_A加密的有效报文。由于B并不知道A的秘密密钥，因而只有当A确实发送过报文时B才可以得到该报文。

有人批评这种签名方法把两种截然不同的功能(即身份验证和保密）混在了一起。在许多应用中，身份验证是必须的，而保密则不是。由于公开密钥加密速度较慢，故希望只发送已签名文件（不需加密）。下面将介绍一种不需要对整个报文加密的身份验证模式。

这种身份验证机制基于单向检验和（one－way checksum）函数 CK的思想。假定有一明文报文P，计算出CK（P）必须比较容易，但从CK（P）几乎不可能找出P，CK（P）应当比报文本身短得多，如只有256位。实际上，有许多具有这种单向特性的数学函数。

要在一明文报文P中签名，发送者A首先计算CK（P），然后用私人密钥将其加密，产生出D_A（CK（P）），最后将[P，D_A（CK（P））]对偶传送到B。报文本身可以用明文发送（或者用公开密钥或传统加密技术加密），后跟加了密的校验和。

当报文及校验和到达B后，B对签名部分（即D_A（CK（P））应用E_A，得到CK（P）。至此，B有3样东西：P、CK（P），以及 D_A（CK（P））。现在 B对 P应用 CK，以看此结果是否与收到的CK（P）一致。若是，则知此报文未遭窜改；若否，则说明报文已被窜改。

如果以后发生争议，B可向法官出示这三样东西，以证明A确实发送过报文P。法官毕竟懂得，即使B能伪造出P和CK（P），并发送过报文P，但B若未得到A的私人密钥就无法伪造出D_A（CK（P））。这种方法的优点是无论报文有多长，只有很短的检验和必须经过费时的公开密钥加密方法加密。

请注意CK单向特征的重要性。如果能从CK（P）得到明文报文P，那么B就可以生成与P具有相同检验和的新报文P’，并把P’、CK（P）以及D_A（CK（P））出示给法官。

虽然上述两种签名方法都相当不错，但它们仍旧存在一些问题。这些问题不是算法本身的问题，而是与算法的运行环境有关。第一，只有当D_A仍是秘密的时候，B才能证明A发送过报文。如果A将其私人密钥公开，这一立论就不再成立；因为任何人包括B都可以发送A所发送的报文。比如说，A和B是两个公司。某个时刻A的经理因为又发现了一个更便宜的供贷商而意识到已发出去的零件订购单不划算。为了否认给原来的那家公司发过订购单，A故意公开其私用密钥，然后告诉警官他们的办公室被盗，密钥被窃走。根据某些地方法规，这家公司不一定要对别人滥用其被盗物品而产生的后果负法律责任。

第二，如果A决定改变他的密钥，将会发生什么情况？这样做显然是合法的，在许多公司里甚至是标准的工作程序。如果发生上述纠纷案，法官对D_A（P）或D_A（CK（P））运用A当前的E_A，结果会发现不能得到P或CK（P）。此时，B会非常难堪。由此可见，需要某种集中控制机制记录所有的密钥变化情况及其日期。

9.1.4　报文鉴别和报文摘要

报文鉴别是一个过程，它使得通信的接收方能够验证所收到的报文（发送者和报文内容、发送时间、序列等）的真伪。

报文鉴别的一种方法是使用报文鉴别码（MAC：Message Authentication Code）。报文鉴别码是用一个密钥生成的一个小的数据块追加在报文的后面。这种技术假定通信的双方共享一个密钥K。当用户A向用户B发送报文M时，就根据此密钥和报文计算出报文鉴别码MAC=F（K，M），这里的F就是加密算法的某一函数。此报文的报文鉴别码和报文一起从用户A传送到用户B。用户B用收到的报文（不包括报文鉴别码），使用同样的密钥K，再计算一次报文鉴别码，并与收到的报文鉴别码相比较。如一致，则鉴别此报文是真的。有不少算法可用来生成报文鉴别码，例如DES算法就可以生成报文鉴别玛，这时可采用密文的最后若干个比特（16或32比特）作为报文鉴别码。显然，对MAC不进行类似加密过程的反向计算，由于鉴别函数的这一特点，鉴别是较难被攻破的。

报文摘要是报文鉴别码的一个变种，将可变长度的报文M作为单向散列函数的输入，然后得出一个固定长度的标志H（M），这个H（M）就称为报文摘要MD。单向散列函数的一个特点是从一个报文生成一个MD代码是容易的，但反过来从一个代码生成出一个报文则实际上是不可能的。另外，它保证不同的报文不会得出同样的MD代码。如果没有这个特性，攻击者就可能用一个伪造报文替代真报文，只要该伪造报文与真报文能够生成同样的MD即可。

我们将许多流行的报文摘要算法（message digest algorithm）通称为MDn，其中n为不同的值。当前使用最广泛的报文摘要算法是MD5。安全散列算法（Secure Hash Algorithm，SHA）是另一个众所周知的报文摘要函数。所有这些函数所做的工作几乎一样，即由任意长度的输入消息计算出定长的加密校验和。

在数学上，报文摘要算法与DES（而非RSA）有更多的共同点。就是说，它们没有正式的数学基础，而是依靠算法的复杂性产生随机的输出来满足对其功能的要求。这里我们

只简要叙述MD5算法。算法本身似乎是一个变换的随机集合，因此它适宜地产生随机的输出也就毫不奇怪了。

图9-1描述了MD4、MD5和SHA的基本操作过程。这些算法每次对512位报文操作，所以，第一步就是要将报文填充为512位的整数倍。这是通过在报文后面填充1到512位来实现的，第1比特为1，其余为0，跟着是64位的整数，它以比特为单位表示原始报文的长度。注意，这允许报文的最大长度为264位。

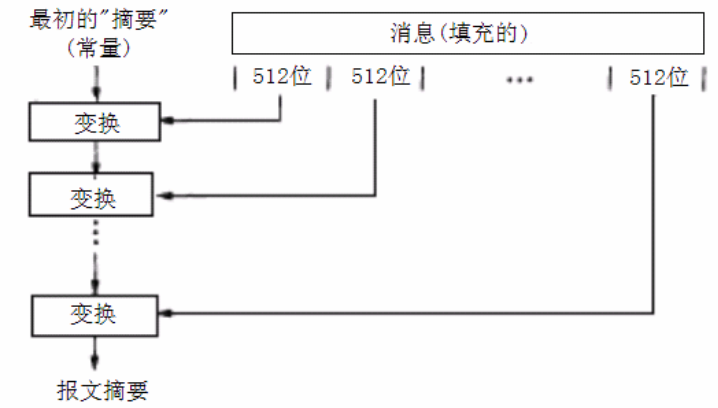


图 9-1　报文摘要的基本操作过程

摘要计算的第1步是把摘要的值初始化为一个常量；然后用以下描述的复杂变换，将该值与报文的第一个512位合起来产生新的摘要值；接着使用同样的变换将这个新值与报文的下一个5l2位结合，以此类推，直到生成最终的摘要值为止。

MD5算法的主要组成部分就是进行变换，取128位摘要当前值作为其输入，加上512位报文，输出一个新的128位摘要。 MD5类似其他现代算法（而不像早期的如MD2的算法），按32位的数量操作，因为在现代处理器中这样做效率较高。因此我们可以把当前摘要值看做4个32位的字（d_0，d_1，d_2，d_3），把要产生摘要的这一段报文看做16个32比特字（从m_0到m_{15}）。

由MD5完成的基本变换可以分为4遍。完成所有这些操作后，原来的（d0，d1，d2，d3）值彻底被搞乱了，即虽然完全依赖于报文字节，但是不提供求那些报文字节是什么的计算方法。现在把搞乱的摘要加到当前这一阶段之前已有的摘要值上，就变成新的摘要值。接着算法对报文的下16个字(512比特)继续进行摘要，直到不再有要进行摘要的字为止。最后一阶段的输出就是报文摘要。

这样得出的MD5代码中的每一个比特，都与报文中的每一个比特有关。Rivest提出了一个猜想，即根据给定的MD5代码找出原来报文的难度，其所需的操作量为2128。到目前为止，还没有任何分析可以证明这种猜想是错误的。MD5已在Internet上大量使用。

安全散列算法SHA和MD5类似，但码长为160位，比MD5多了32位。它也是用512位长的数据块经过复杂的运算得出的。SHA比MD5更安全（多了一个232的因子），但却比MD5要慢些。SHA是美国政府的一个标准。

值得指出的是，网络管理的著名协议SNMPv2就采用了一种MD鉴别技术。在该MD鉴

别技术中，通信双方共享一小段秘密的数据块，发送端先将此秘密数据块追加在报文M的前面，然后输入到散列函数H，计算出MD，然后将MD追加在M的后面，同时去除一开始加上的秘密数据块，接着就发送给接收端。接收端先去除加了密的MD，然后在报文M的前面追加上自己拥有的秘密数据块后，输入给散列函数H，计算H（M）。比较H（M）和MD，若一致，则收到的报文M是真的。

9.1.5　IPv6对网络安全性的支持

现在人们普遍地重视IP网络的安全性。IPv6设计者意识到必须在新一代的IP协议中加进严肃的安全功能。这些安全特征将成为促进IP向新协议转变的关键诱因。事实上，这种努力的结果产生了对IP级身份验证和加密过程的定义。这些过程对IPv4和IPv6都适用。它们必须对IPv4向后兼容，但在IPv6产品的初始阶段就必须被实现。

9.1.5.1　加密和身份验证

IPv6规范包括对两个安全载荷的描述：身份验证头和加密安全载荷。一个扩展头提供身份验证，该过程使得分组的接收方可以相信源地址通过了身份验证处理，而且分组在传输的过程中没有被篡改。另一个扩展头保证只有合法的接收方能够阅读报文的内容。这两个机制都是基于安全关联的概念。

身份验证和加密需要发送方和接收方就一个密钥、一个身份验证或加密算法以及诸如密钥的生命期或算法使用的细节等一组辅助参数达成一致。这一套协定构成在发送方和接收方之间的安全关联。在接收分组的时候，仅当接收方能够把这些分组跟一个安全关联的上下文相联系的时候，它们才能被验证或解密。IPv6经过身份验证和加密的分组都传达一个安全参数索引(SPI)。

当分组通过一个单播地址发送到一个惟一的接收方时，SPI(安全参数索引)由这个接收方选定。例如，它可以是对于由这个接收方维护的一个安全上下文列表的索引。事实上，主机的每个通信对方所使用的SPI（安全参数索引）是安全关联的一个参数。每个站必须记住它的通信对方所使用的SPI，以便鉴定安全上下文。

当把分组通过一个多播地址发送给一组接收方时，SPI对该组的所有成员是通用的。每一个成员都能够把组地址和SPI的结合跟密约、算法以及其它参数相联系。SPI一般是作为密钥交换过程的一部分商定。

身份验证头（AH）是一个为IPv6定义的类属扩展头。它以载荷类型51表征，典型地插在IPv6头和端到端载荷之间。例如，经过身份验证的TCP分组包含一个IPv6头、一个身份验证头和TCP分组本身。在这里，可能有多个变种，例如把一个路由选择头插在AH的前面，或者把端到端的选项插在AH和载荷之间。

身份验证头的存在并不会改变TCP的行为，事实上也不会改变诸如UDP或ICMP这样的其它端到端协议的行为。它只是为数据的源提供明确的保证。端到端的协议可以被指示拒绝任何未经适当的身份验证的分组。

身份验证头有一个非常简单的语法。如图9-2所示，开头96位包含在菊花链中的下一个

头号码、身份验证载荷的长度、应该置成0的16个保留位、安全关联的32位SPI (安全参数索引)和一个32位的序列号。这一组固定长度参数后随身份验证数据，编码成可变数目的若干个32位字。长度定义为后随SPI的32位字的数目(包括1个32位的序列号)。例如，如果身份验证数据是96位长，那么长度将设置成4（=1+3）。

图 9-2　身份验证头的格式

发送方对在安全关联上发送的分组编号。接收方使用这个号码识别和丢弃老的分组。这样做可以阻止“重复操作”攻击。在称作重复操作的攻击中，黑客得到一个经过身份验证的有效分组的一个拷贝，进行重复操作。不过在实现IPv6的这一保护机制时应该小心，因为Internet并不保证对分组的有序投递。接收方应该把在一个经过正确的身份验证的分组中接收到的最高序列号N跟安全关联相联系。他们还应该维持布尔量数组，表明是否已经收到编号在N-W和N之间的所有分组。在缺省的条件下，窗口尺寸W设置成64。

需要注意的是，如果序列号允许循环，那么它不能够完成保护接收方不受重复操作的攻击。在使用关联发送多于232个分组的条件下，就会发生这样的问题。为取得更好的安全性，在这样的问题发生之前就应当协商一个新的密钥。

身份验证数据从对密码检验和的计算产生。该计算涉及载荷数据、IPv6头和扩展头的一些域以及由关联成员共享的秘密。身分验证数据的精确长度取决于所选的计算检验和的算法。接收方基于分组的内容和由SPI索引的秘密计算一个期待值，然后把计算的结果跟在分组中收到的身份验证数据比较。如果两个值相同，那么他就可以断定，分组的形成者知道秘密，分组在传输的过程中没有被修改。

使用身份验证头可以防止地址欺骗，也可以保护用户免于被盗用连接。在计算身份验证数据之前，发送方必须准备一个特别版本的报文，该报文独立于被传送的报文。

- 在IPv6头中，开头32位（版本，类别，流标记）被排除在计算之外。
- 在IPv6头中，跳段计数设置成0。
- 如果使用路由选择头，把IPv6目的地址设置成最终目的地，把路由选择头的内容设置成分组到达时应有的值，并相应地设置地址索引的值。
- 在计算检验和时不考虑C位置1的选项。它们的内容用一组0字节代替。

检验和的计算使用密码算法。在IP安全体系结构中建议的算法是带密钥的MD5。MD5使用非线性变换为报文计算128位的检验和，该变换使得反向推导非常困难。带密钥的MD5的运算把报文跟一个密钥结合在一起，然后再计算非线性变换的哈希值。把密钥前置和后置到报文以防止某种类型的攻击。

检验和的计算的确切顺序如下：

- 通过置0跳段计数和传输过程中需要改变的选项，以及形成路由选择头的最后目的地版本，从报文M得到独立于传输的版本M’。
- 由于MD5对16字节块（128位）进行计算，所以 对M’做0字节填充，以满足下一个16字节边界条件。（密钥K也应做0字节填充，使得满足下一个16字节的边界条件。）
- 用0字节填充密钥K，得到一个64字节串，然后把那个串跟一个由64个相同字符值0×36（十六进制）组成的常量串异或，得到一个64字节的串K1。
- 把K1跟待做身份验证的报文串接，再计算这个串的MD5检验和（128位）。
- 通过用字节填充密钥K，得到一个64字节串，然后把那个串跟一个由64个相同字符值0×5C（十六进制）组成的常量串异或，得到一个64字节的串K2。
- 把K2跟K1的16字节（128位）MD5检验和以及报文串接，计算这个串的MD5检验和（128位）。
- 保留MD5检验和串的开头12个字节（96）位。

把检验和截尾成96位的目的是把AH的大小保持在24字节(8字节的整数倍)，同时也没有过分地减弱身份验证的功能。

事实上，身份验证算法是作为安全关联建立的一部分进行协商的。MD5算法仅仅被指定为一个默认算法，保证所有的实现至少使用一个通用的算法。未来完全可以使用其它的算法，要么计算起来更快，要么比MD5更难攻破。

身份验证头并不变换数据，数据依然是明文。当需要保密的时候，应当使用加密安全载荷（ESP头）。如图9-3所示，这个头总是放在IPv6扩展头菊花链的最后位置。

图 9-3　使用 ESP 头的加密分组

图 9-4　加密安全载荷的类属格式

ESP头也包括一个序列号和一个身份验证数据（参见图9-4）。ESP的序列号跟AH的序列号相似，它保护接收方免遭重复操作攻击。放在加密数据后面的身份验证数据（检验和）保护接收方免受毁坏或截短加密数据一类攻击。用以计算该检验和的算法是安全关联的一

个参数。在所有的情况下，该检验和都要保护序列号和加密数据。

确切的格式依赖于所使用的特定加密算法。规范建议的缺省算法是数据加密标准（DES）的密码块（Cipher Block）连接(Connection)方式（DES-CBC）。如图9-5所示，当使用DES-CBC时，加密数据以可变长度的初始向量（IV）开头，后随载荷的加密值本身，一些填充字节，填充长度指示和载荷类型。

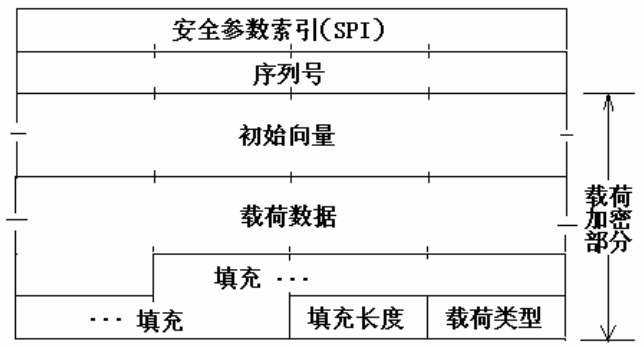


图 9-5　使用 DES-CBC 的 ESP 载荷格式

使用填充长度是为了使报文在一个64位字边界处结束。填充字节可以包含任意值。在加密报文中的最后一个字节表示载荷类型，例如TCP。它的前一个字节表示填充的数量。

初始向量由可变数目的32位字组成。确切的数目定义为安全关联的一个参数。初始向量的内容通常是由一个随机数发生器产生的结果。初始向量的作用是保证报文的开头几个字不可预测，保证黑客不能够使用基于对明文和加密值的了解的攻击方法。借助该算法，随机性被传播到报文的其余的字。

DES-CBC仅仅是一个缺省算法，在建立安全关联时可以选择其它的算法。

身份验证和保密是两种不同的服务。一种服务保证报文来自正确的源，并且没有被篡改。另一种服务保证报文不会被第3方听懂。大多数加密方法都提供某种报文源指示。当报文没有使用正确的密钥加密或解密时，加密算法在产生随机位方面的效果是相当好的，因此只要进行一些语义上的检查就足以确定加密是否成功。然而这并非完全的保证。黑客通过结合先前编码的报文可以执行一些微妙的攻击，使得解密的结果看来是正确的，虽然这并不可靠。

当需要强身份验证和保密性时，可以依赖在一个结合型保密和身份验证载荷中的身份验证检查，或者同时使用AH和ESP。在这种情况下，建议总是把ESP放到AH的“内层”，即把ESP头放到AH头的后面，这就使得接收方要么在试图解密之前先检查身份验证，或者平行地做身份验证和解密。

9.1.5.2　密钥分发

安全关联的建立依赖只为关联成员所知的密钥的存在。有效的安全性设施依赖有效的密钥分发方法的存在。在密钥管理和安全协议之间的联结是安全关联的安全参数索引。密钥管理过程不仅提供密钥，而且也提供安全关联的其它参数。

Internet团体就密钥分发方法达成一致看来是一个缓慢的过程。在已经提出的议案中，

有一些是基于Whitfield Diffie和 Martin Hellman提出的密钥交换算法。在此有必要对此算法作一介绍。

在原始的Diffie-Hellman算法中，两方A和B就一个质数p和一个生成元g达成一致。A方选取一个随机数x。它计算值n = g. x mod p ,把它发送给B。B再选取一个随机数y,计算值m = g.y mod p ,并把它发送给A。在这一阶段，A知道m和x，B知道 n和y。而第三方可能知道m或n, 他们不能够得到x或y。A和B可以计算会话密钥：

Z=n.y mod p = m.x mod p = g.x.y mod p

这个双方共享的密钥随后可以用于加密或身份验证。

在可以被普遍接受的标准形成之前，早期的采用可能要依靠手工的密钥分发。特殊的情况是多播，它需要特别的算法。

多播提出了一个困难的问题，因为一个组的所有成员都得到同样的密钥。上述用于单播的解决方案不是很有用，因为由密钥变换完成的算法产生跟随机值有关的选择。

组密钥的分发将必须依赖一个密钥服务器。然而使用常规的密钥交换过程在组成员和组的密钥服务器之间建立安全关联是完全合理的。

9.1.6　无线局域网的有线等价加密WEP

在无线局域网中，数据传输是通过无线电波在空中广播的，因此在发射机覆盖范围内数据可以被任何无线局域网终端接收。因为无线电波可以穿透天花板、地板和墙壁，所以它可以到达不同的楼层甚至室外等不需要接收的地方。安装一套无线局域网就好像在任何地方都放置了以太网接口，因此无线局域网使数据的保密性成为人们关心的重要问题，因为无线局域网的传输不只是直接到达一个接收方，而是覆盖范围内所有终端。IEEE 802.11规定了一个加密服务选项解决了这个问题，将IEEE 802.11网络的安全级提高到与有线网络相同的程度。IEEE 802.11规定了一个可选择的加密机制称为有线等效加密，即WEP。WEP提供了无线局域网数据流安全方法，它是一种对称加密，加密和解密的密钥及算法相同。

WEP的目标是：

（1）接入控制。防止未授权用户接入网络，他们没有正确的WEP密钥就会被拒绝访问。

（2）加密。通过加密和只允许有正确WEP密钥的用户解密来保护数据流。

该加密功能应用于所有数据帧和一些认证管理帧，可以有效地降低被窃听的危险。

WEP利用密码来实现保密目标的同时，还可以成为身份验证机制，这就是共享密钥认证。站点通过共享密钥进行加密认证，加密算法就是有线等价加密WEP。全部报文都使用检验和加密，提供了一定的抵抗篡改的能力。

WEP有三种实现方式：无加密、40位加密和128位加密。很明显，无加密意味着没有保密性，数据以明文形式传输，任何能够访问WLAN中RF的无线嗅探器应用程序都能观察这些传输内容。40位密钥实际上是10个十六进制数字，还附加了一个24位的初始化向量（IV ），所以有时候也说成是64位。128位密钥也是相同的处理过程，它包括一个104位密钥（26个十六进制数字），然后再添加了24位的初始化向量（IV ）。在40位密钥和128位密钥的两种情况下，位数越大，加密强度越大。

WEP使用RC4算法，该算法是由Ron Rivest(即RSA中的R)开发的一种流密码。发送者和接收者都使用流密码，从一个双方都知道的共享密钥创建一致的伪随机字符串。发送者使用流密码对传输内容进行异或（XOR）操作，产生密文，接收者获得共享密钥和相同的流密码，然后用同样的异或操作来获得原来的传输内容。

初始化向量用来创建相同的密码流，即在 IV和密钥相同的情况下，产生的流密码就是相同的。IV由发送者生成，并包含在每帧的传输内容中。每帧都使用不同的IV，避免密钥的重用会减弱机密的效果。

大多数的基站（AP）都使用至少40位加密的WEP，但通常还支持128位选项。对于公共网络，应该具备128位加密功能。另外在安装和启动之后，应立即更改WEP密钥的缺省值。在试图同网络连接的时候，客户端的SSID和密钥必须同AP匹配，否则将会失败。 SSID（服务组标识符）是一个无线局域网子系统内通用的网络名称，它服务于该子系统内的逻辑网段。最理想的方式是WEP的密钥能够在用户登录后进行动态改变，这样黑客想要获得无线网络的数据就需要不断跟踪这种变化，难度就大了。

IEEE 802.11定义的共享密钥认证是先假定每个站点通过一个独立于IEEE 802.11网络的安全信道，已经接收到一个共享密钥，然后这些站点通过共享的密钥进行加密认证，加密算法就是有线等价加密（WEP）。

9.1.7 网络安全技术的应用

9.1.7.1 PEM

保密增强邮件（PEM：Privacy Enhanced Mail）是IETF早期为因特网电子邮件制定的一个支持加密、身份验证及报文完整性的机制。PEM在一组4个RFC（在1993年完成）文档中规定了：

- 使用PEM的报文格式
- 认证机构的分层结构
- 所使用的一组加密算法
- 请求和吊销证书的报文格式

在电子邮件的安全通信中有几个颇具挑战性的问题。首先，多数电子邮件系统期望消息只含有ASCII字符，而加密算法通常输出二进制数据。其次，一个电子邮件报文通常要经过许多系统，这些系统关于文本行多长以及怎样确切表示一行的结束都有各自的概念，比如，只用＜CR＞（回车）字符或用＜CR＞后跟着＜LF＞（换行）表示一行。对报文进行的简单修改，如把一个长行分成两行，对一个普通电子邮件报文的内容没有太大影响，但可能使已签名的消息对接收者来说变得无效。PEM解决了这些问题，它们恰好是在发明MIME时就需要解决的问题。

最后，电子邮件报文常常要被发送给大量的接收者，也许要经由一个执行邮件列表名“扩展”的机器。我们需要一些程序，通过这些程序，这样的报文就可以被安全地发送到所有的接收者。

也许PEM最独特的一面就是其认证分层结构。PEM使用RSA公开密钥技术加密和验证，

因而需要一种机制将公开密钥可靠地分发给参与者。回顾一下当参与者A希望得到参与者B的公开密钥时，一种方法就是从被A信任的、称为认证机构的某个实体获得一个证书。实际上，这个证书指出，“B的公开密钥是K，是由CA签发的”。而PEM不依赖一个集中的管理机构（集中管理的可扩展性不好），它指定一个如图9-6所示的CA的树形分层结构。树是分发证书的一种方式。

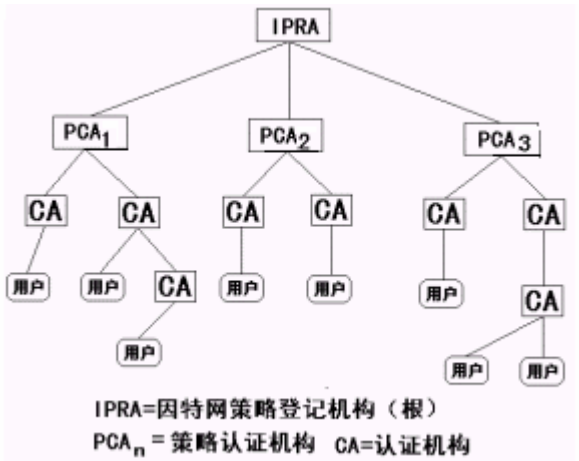


图 9-6　用于 PEM 的认证机构的树形分层结构

为了使认证过程可扩展，PEM认证机构能把它的权力授予树中低层的另一个CA。即CA_1不是为个体签署证书，而是为其他CA，如CA_2签署证书。假如知道CA_1的公开密钥，就可以可靠地得到CA_2的公开密钥。因此，如果现在CA_2给B签署了证书，就可以确信这确实是B的公开密钥。通过反复地授权，可以建立一个像图9－4中所示的树。只要从一个根CA的公开密钥出发，就可以使用一个证书集合获得这个树上任何叶子的公开密钥。

然而，这种授权方法的问题在于，把信任授权从一个CA传给另一个CA。CA_1签署了CA_2的证书这一事实可以让我们确信拥有CA_2的一个合法公开密钥（因为信任CA_1所做的工作），但这并不能使我们信任由CA_2发行的证书，因为CA_2也许是由足够金钱作为交换来签署任何证书的罪犯来运营的。要处理这个问题，根认证机构IPRA（The Internet Policy Registration Authority，因特网策略登记机构）就不仅需要知道那些CA的身份，而且要了解其更多的信息。例如，IPRA需要知道CA使用什么过程确保其证书是有效的。

因为不同CA可以确定其证书有不同的有效期长度，所以PEM分层结构允许不同类型的CA，这些CA是由不同的策略认证机构（policy certification authorities， PCAs）认证的。当对PCA下面的CA授权时，每个PCA公布一套它所遵循的策略，并要求那些CA也去遵循。这样，假定图9-4中的PCA1有非常严格的策略，那么由PCA1下面的CA发布的任何证书的有效性就有很高的可信度。相反，当我们收到一个由树中不太严格的PCA下面的CA发布的证书时，我们可能愿意相信发布证书的机构是正确的，但是也可能会对证书指定的个体的身份有一些怀疑。

PEM证书遵循X．509标准。当A需要传送其公开密钥给B时，他应具有足够的证书使B确信该密钥是正确的。这样，如果A和B为同一组织工作并共享同一CA，则A可以只传送由

本地CA发出的证书。在极端的情况下，如果A和B彼此对另一方一无所知，那么A可以发送从树根（IPRA）到A整个路径上的一条完整的证书链。

当A希望验证一个报文并把它传送到B时，A计算该报文的加密校验和（通常使用MD5），然后用A的私有密钥签署MD5校验和。A发送报文：

m+E（MD5（m），$private_A$）

其中m是原始的报文。报文的接收者用A的公开密钥去解密签名的校验和；他也对收到的报文计算MD5校验和。如果两个值匹配，那么证明消息在传送途中未被修改，且证明它是由A发来的。要注意的是，接收者唯一需要对报文进行验证的是A的公开密钥，因此这个过程能很容易地被该报文的任意多个接收者应用。

9.1.7.2 PGP

良好保密性（PGP： Pretty Good Privacy）是为电子邮件提供加密和鉴别功能的另一个方法。它与PEM在很多细节方面有所不同（例如，报文格式和加密算法），但最主要的区别是PGP处理证书的方法。与PEM实施一个证书的严格分层结构相反，PGP允许证书任意地结网。这对PGP的使用已有很重要的积极影响。

回顾公开密钥分发的基本问题就是建立一个信任链。PGP确认每个用户有它自己的全套标准，按这套标准每个用户应该信任由其他人证明的密钥。比如，假定一个我很熟悉的人A，亲自把他的公开密钥给我，那么我会非常确信这真的就是他的公开密钥。但如果A给我的是由A签名的、关于B的证书，我可能希望知道是否A是一个由金钱作交易、签署虚假证书的家伙，或是否他草率地检验了真的就是B而不是其他什么人要求他签署证书。我可以信任A为一些人签署的证书（比如，他的同事）但不信任他为另一些人（例如，政治家）签署的证书。显然随着信任（或不信任）链不断变长，事情也变得越来越糟。

PGP允许证书关系形成一个任意的网，而不强制一个严格的证书的分层结构。此外，它允许每个用户自主决定他们希望放在给定的证书中多大的信任度。例如，假设你有一个由A提供的B的证书；那么你可以给该证书指定一个适度的信任级。但是，如果你有另外一个由C和D给你提供的B的证书，他们是适度可信赖的，那么就可以大大增加你具有的B的公开密钥的信任等级。简而言之，PGP认为建立信任的问题完全是个人的事情，而且给用户未处理过的资料让他们做出自己的决定，而不是假设他们都自愿信任单一层次的CA结构。引用PGP的开发者Phil Zimmerman的话来说，“PGP是为喜欢自己包装降落伞的人设计的。”

PGP在网络界已经相当流行。PGP密钥签署集会是IETF会议的一个常规特征。在这样的聚会上，个人可以：

- 从他知道其身份的其他一些人中收集公开密钥
- 把他的公开密钥提供给其他人
- 获得由其他人签署的他的公开密钥，从而收集对不断扩大的人群有说服力的证书
- 签署另外一些人的公开密钥，这样帮助他们建立起他们能够用来分发其公开密钥的一套证书。
- 从他信任的足以签署密钥的其他人那里收集证书

因此随着时间的推移，一个用户会收集一套具有不同信任度的证书，PGP把这些证书存储到一个称为密钥环的文件中。

现在假定用户A希望发送一个报文给用户B并对B证明其真的来自A。PGP处理这个问题的方法几乎与PEM一样。首先，报文体本身或用一种防止电子邮件网关修改它的保护方式编码，或用一种透明的方式发送。然后A在报文体上建立一个加密校验和（例如，使用MD5），再用A的公开密钥加密该校验和。（PGP允许使用各种不同的加密算法并说明在该报文中使用哪一种算法。）

一旦接收到报文，B就使用PGP的密钥管理软件在他的密钥环上查找A的公开密钥。如果没找到，B当然不能验证该报文的可靠性。如果找到了该密钥，就计算收到的报文的校验和，用A的公开密钥解密收到的加密校验和，并比较两个校验和。如果相同，B知道A发送了这个报文而且A签名后未被更改。除了提供签名验证的结果外，PGP根据已有的A的证书数量及签署该证书的人的可信赖度，告诉B他以前赋予这个公开密钥的信任级。

报文的加密也和PEM相似。随机地挑选每个报文密钥用DES这样的对称算法来加密该报文。每个报文密钥用接收者的公开密钥加密。PGP从A的密钥环上得到这个密钥并通知A他指定给该密钥的信任级。为了防止报文被邮件网关损坏，报文被编码再发送到B。当收到时，B使用他的私有密钥解密每个报文密钥，然后再用相应的算法去解密该报文。

PGP允许为不同功能使用不同的加密算法。在一个报文中实际使用的算法在头部（标题）字段中说明。除在邮件报文中放置这些信息外，PGP允许用户在包含其公开密钥的文件中列出他推荐的算法。因此，有该用户的公开密钥的任何人都会知道在给他发送时使用哪一种算法最安全。

构造一个与协议无关的安全系统是一个非常好的想法，因为你决不知道什么时候喜欢的算法会被证明不足以健壮到能达到你的目的。如果你能很快地改变到一个新的算法而不必改变协议描述或实现，那样就非常好。

9.1.7.3　S-HTTP

S-HTTP是Web上使用的超文本传输协议（HTTP）的安全增强版本。它提供了文件级的安全机制，因此每个文件都可以被设成保密/签字状态。用于加密及签名的算法可以由参与通信的收发双方协商。S-HTTP提供了对多种单向散列函数的支持，如MD2，MD5及SHA（安全散列算法）；对多种私钥体制的支持，如DES、三重DES以及RC4等；对数字签名体制的支持，如RSA和DSS（数字签名标准）。S-HTTP对单个文件作“保密/签名”的区分，而作为传输层安全机制的SSL（安全套接层协议）则把参与通信的相应过程之间的数据通信通道按“保密”和“已认证”进行监督。

9.1.7.4　DNSsec

1994年IETF建立了一个工作组，研究DNS服务器的安全问题，其工作结果产生了安全DNS，即DNSsec。

DNSsec在概念上非常简单，它基于公开密钥加密算法。每一个DNS区域都有一个公钥/私钥对。由DNS服务器发送的所有信息都用源区域的私钥签字，因此接收方可以验证其身份。

DNS服务器提供3项主要服务：验证数据的来源、公钥发布以及对事务处理和请求的身份验证。第1项服务验证返回的数据已得到区域拥有者的认可。第2项服务用以安全地存储和检索公钥。第3项服务可以防止反演和欺骗攻击。

9.2 基本练习题

1. 试述网络安全的特征。

答：安全特性是基于ISO 7498-2的安全服务与安全机制。不同安全策略、不同安全等级的系统有不同的安全特性要求。

安全服务与安全机制指的是基于OSI的安全体系结构实现安全通信所必要的服务以及相应的机制。ISO 7498-2描述了5种可选的安全服务：身份鉴别、访问控制、数据保密性、数据完整性和不可否认性。与上述5种安全服务相关的安全机制有8种：加密机制、访问控制机制、数字签名机制、数据完整性机制、身份鉴别（认证）机制、通信业务填充机制、路由控制机制、公正机制。此外，还有与系统要求的安全级别直接有关的安全机制，如安全审计、可信功能、安全标记、事件检测和安全恢复等。

2. 根据著名的Gartner公司的研究部门关于灾难发现和恢复的可能性研究报告，下列哪一个陈述是正确的？

a. 遭遇灾难的10个企业中有2个在2年内被淘汰。
b. 遭遇灾难的5个企业中有1个在1年内被淘汰。
c. 遭遇灾难的5个企业中有3个在5年内被淘汰。
d. 遭遇灾难的5个企业中有2个在5年内被淘汰。

解答：d. Gartner评估，遭遇灾难的5个企业中有2个在5年内被淘汰。仅当在灾难发生之前和之后采取必要的措施，企业才能改善其成功的可能性。

3. 下列哪些事项可以被看成是对公司网络威胁的可能来源？

a. 投递和收集邮包的日常信使人员。
b. 心怀不满的离开公司的前职员。
c. 业务出差到另一城市参加会议的雇员。
d. 有一个组织向管理楼房的公司租用了一个办公室，并决定安装一个消防系统。

解答：a. b.c. d. 所有这些事项都可能产生威胁公司网络的条件。常规的信使服务人员跟雇员熟悉，雇员可能不会留心因投递人员进入服务器房间而可能发生的安全问题。即使有很好的离职补偿，由于裁员而丢失工作的雇员还可能是恼火的。外出的雇员也许不会产生威胁，但如果该雇员携带一个笔记本计算机，其中包含私有信息或保存有口令的浏览器，如果该笔记本计算机被盗，黑客就有了访问网络的强大工具。安装消防系统是个好举措，但如果该系统失灵，公司的服务器、计算机和其它设备被水或火破坏，从这样的灾难中恢复就会很困难。

4. 说出安全策略应该考虑的至少6个方面的问题。

解答：（1）授权　（2）责任　（3）数据可提供性　（4）数据完整性　（5）数据保密性　（6）保护隐私

5. 为什么说奇偶位、检验和以及CRC并不能提供安全性？

解答：奇偶位、检验和以及CRC并不能保证到达接收方的数据真地来自所标示的发送方。你不可以依赖这些机制来保证所传输数据的完整性，因为非授权用户可能从传输媒体上截获分组，修改其内容和奇偶位、检验和或CRC值，然后再放到传输媒体上继续向前传送给接收方。

6. 什么是DOS攻击？

解答：DOS(Denial-of-Service)攻击用大量非接收方希望接收的分组淹没网络，使得受到影响的系统不能正常工作。DOS攻击最常见的形式是SYN攻击。攻击者突然在短时间内给一个系统发送大量的SYN分组，使得系统花费所有的时间来满足所有的TCP连接请求。

7. 假冒的含义是什么？

解答：假冒是指修改分组的源地址，使得看起来好像是从另一个源发送的。

8. 什么是替换密码？

解答：替换密码是一种加密机制，它把实际的字母或符号用另一个字母或符号替换。

9. 替换密码的主要问题是什么？

解答：替换密码隐藏报文的实际字符，但它并不隐藏在报文中各种字符出现的频率或图案。

10. 什么是转置密码？

解答：在转置密码中，明文的实际字符被保留，但字符被重新排序。

11. 什么是DES？

解答：DES的基本概念是对明文按照64位的块方式做替换密码加密，使用64位的密码参数，其中仅56位真正用于密钥。

12. 在公钥加密系统中，发送方用接收方的公钥加密报文。接收方使用什么密钥解密报文？

a. 接收方的私钥
b. 接收方的公钥
c. 发送方的私钥
d. 发送方的公钥

解答：a. 接收方的私钥。当报文用一个公钥加密时，可以解密报文的仅有的密钥是同一组密钥中的私钥。因此，当报文用接收方的公钥加密时，接收方仅仅可以用它的私钥解

密。

13. 什么是RSA？

解答：RSA典型地使用512位的密钥，它需要比DES多得多的计算能力。RSA的安全性是基于对大数的因式分解。由于加解密所需要的计算能力和时间，RSA加密是很难攻破的。

14. 但做数字签名时，使用什么密钥加密签名？

解答：在数字签名的情况下，报文用发送方的私钥加密，接收方用发送方的公钥解密报文，因为仅仅发送方有其私钥，如果接收方可以用发送方的公约解密报文，那么接收方知道该发送方是真实的。

15. 通常用于数字签名的身份验证协议是什么协议？

解答：是Kerberos。该名字来自希腊神话中的一个多头狗，它守卫通往地狱的大门。Kerberos在开放的网络上提供对用户和服务器的身份验证。验证过程如下：

客户向身份验证服务器（AS）发送请求，请求一个给定的服务器的身份证明文件。作为应答，AS把被请求的证明文件用客户的密钥加密后发送给客户。证明文件由下列两部分组成：（1）该服务器的资格证明书　（2）暂时的密钥（通常称作会话密钥）。

身份验证服务器（AS）维持一个关于用户和服务器以及他们的密钥的数据库。在收到AS的应答后。客户把得到的资格证明书传送给服务器，在报文中包含该客户的ID和会话密钥的一个拷贝，并且用该服务器的这个密钥加密。会话密钥（现在由客户和服务器共享）被用来验证客户的身份，并且可选地被用来验证服务器的身份。它也可以被用来加密在客户和服务器之间更多的通信，或者用以交换一个分立的子会话密钥，用以加密更多的通信。

16. 在X.509安全证书中必须定义哪4个必须的内容？

解答：下列域是在一个X.509安全证书中必需的：

- 为其设公钥的组织、公司或实体的名字。
- 在证书中标出的这个组织、公司或实体的公钥。
- 授予公钥证书的机构的名称。
- 数字签名。

17. 浏览器证书的主要目的是什么？

解答：浏览器证书保证接收方将得到另一方公钥的可靠拷贝。一旦在用户的浏览器中安装了证书，web服务器就可以使用它自己的私钥验证来自用户的报文。为你的浏览器下载一张证书将允许你得到对Web站点安全的访问，允许Web服务器确定你是被信任的，可以获得在它的站点上的信息。

18. 把数字签名和公钥加密一起使用的优点是什么？

解答：结合使用数字签名和公钥加密，你可以投递机密报文，并验证发送方是真实的。

19. 用于安全数据传输的隧道是怎样工作的？

解答：用于安全数据传输的隧道是一种在IP 中的IP的隧道，它是使用VPN建立一条通过Internet的专用连接。在VPN网络一端的整个外出分组都被加密，包括头和所有数据并把一个未加密的头加到这个分组上，该未加密的头包含发送方VPN系统（路由器）的地址信息和在另一端的接收方VPN系统（路由器）的地址信息。在这个附加的头内没有除这两个VPN机器之外的其它机器的地址或IP号码。接收方解密分组的加密部分，然后把它转发给在那里附接到VPN的网络。

20. IP端口有哪3种类型？

解答：（1）周知端口。这些端口号是由IANA分配的，在大多数系统中，它们仅可以由在操作系统中的特权级的进程或服务使用。周知端口的号码范围是从0到1023。（2）注册端口。这些端口跟IANA登记，并被大多数的应用和用户使用。注册端口的号码范围是从1024到49151。（3）动态的或专用端口。这些端口可以由任何程序和任何人使用。它们典型地由访问一个服务的客户使用。由于客户不运行服务，在客户方使用的端口号不相干。

21. 用一句话描述防火墙的概念。

解答：防火墙的概念是仅允许被准许的交通离开网络和仅允许被准许的交通从外界进入网络。

22．分组过滤执行什么样的任务？

解答：分组过滤的主要工作过程是由防火墙检查在分组中的头信息。防火墙可以检查源和目的地IP地址，如果号码或对应的网络是在被允许的列表中，那么分组可以通过防火墙。基于IP地址的分组过滤运行在OSI协议栈的网络层或第3层。

23. 应用网关的含义是什么？

解答：提供OSI上层过滤的防火墙有时也称作应用网关或代理。

24. IPsec AH 提供什么功能？

解答：AH即IP身份验证头提供访问控制、身份验证、无连接报文完整性和防止重演保护。

25. IPsec有哪3个主要特征？

解答：（1）模块性。安全管理员可以选择一种加密算法和安全协议。（2）安全服务。有许多安全服务可供管理员选择。这些服务包括访问控制、报文完整性、身份验证、可以使分组不能够从非授权用户再次发送的防止重演保护，以及保密性。（3）安全服务应用的详细级别。管理员可以选择对所有的分组施加限制，以满足一个特定的标准；或者基于其它的因素仅对分组的一个子集施加限制。

26. 什么是IPsec SA？

解答：两个使用 IPsec的实体（主机或路由器）在交换数据之前，必须首先建立某种约定，双方需要就如何保护信息、交换信息等公用的安全设置达成一致，更重要的是，必

须有一种方法，使那两个实体安全地交换一套密钥，以便在它们的通信中使用。这种约定，称为安全关联（SA：Security Association）。SA是一个单向的逻辑连接，也就是说，在一次通信中，IPsec 需要建立两个SA，一个用于入站通信，另一个用于出站通信。若某个实体，如文件服务器或远程访问服务器，需要同时与多台客户机通信，则该服务器需要与每台客户机分别建立不同的SA。如果在交换信息的两个实体之间同时使用AH和ESP，那么需要有4个SA。

27. IPsec ESP提供什么功能？

解答：ESP即封装安全载荷头提供访问控制、身份验证、无连接报文完整性、防止重演保护和保密性。

28. HTTPS使用的缺省端口是什么？

解答：当HTTP结合TLS（运输层安全性）使用时，它被称作HTTPS（Secure HTTP），对应的URL表达式也由http改成https,例如https://www.ict.ac,cn。HTTPS使用的缺省端口号是443。

29. 什么是VPN?

答：VPN（虚拟专用网络）是一种软件，由两个组织在用以通过Internet互连的设备上运行。VPN软件起的作用像是包过滤器，允许仅一个VPN设备向VPN软件所配置的另一个VPN设备传输。VPN执行的第二个任务是在数据通过VPN链路传输之前将其加密。在技术特征上，VPN综合了专用网络和公用网络的优点，允许有多个站点的企业拥有一个假想的完全专有的网络，而使用公用网络作为其站点之间交流的平台。在本质上，VPN是将物理分布在不同地点的网络通过公用骨干网（尤其是因特网）连接而成的逻辑上的虚拟子网。简言之，它是一种建立在开放性网络平台上的专有网络。VPN的定义允许一个给定的站点是一个或者多个VPN的一部分，在这种意义下，VPN可以是交叠的。为了保障信息的安全，VPN技术采用了身份鉴别、访问控制、保密性和完整性等措施，以防止信息被泄露、篡改和复制。

30. PGP提供的4个特征是什么？

解答：PGP（颇好保密性）提供下列特征：
（1）保密　　（2）身份验证　（3）数字签名　　（4）压缩

31. PEM是怎样工作的？

解答：PEM（保密增强邮件）首先把报文转换成规范的格式，使得所有的报文对于空格、回车和换行都具有同样的格式。使用MD5或MD2产生该报文的散列值。把原始报文跟散列值串接在一起，使用DES加密。将加密报文用Base64编码，并以MIME格式的电子邮件报文形式发送给接收方。

32. 什么是ISAKMP?

解答：ISAKMP（Internet安全关联和密钥管理协议）是IPsec的重要组成部分，它指定

对安全关联（SA）的设立和配置，其参数包括建立、协商、修改和删除SA的分组的格式。尽管ISAKMP也涉及密钥交换，但并没有指定必须使用哪种特别的密钥交换协议。最常使用的密钥交换协议是IKE（Internet密钥交换协议），它被用来处理加密密钥的分发问题。IKE建立一个专用的经过身份验证的密钥管理通道，两个对等实体使用这个通道通信，就将要使用的加密、身份验证和压缩算法达成一致。

33. IPsec有哪两种使用方式？

解答：运输方式和隧道方式。运输方式就在IP头的后面插入IPsec头。在IP头中的协议域杯被改变成表明有一个IPsec头后随常规的IP头（在TCP头的前面）。IPsec头包含安全安性信息，主要有SA标识符、一个新的序列号和可能的对于载荷的完整性检验。

在隧道方式中，整个IP分组（头和所有内容）都被封装在一个具有全新的IP头的新的IP分组中。当隧道在非最终目的地的位置结束时，就可以使用隧道方式。在一些情况下，隧道的端点是安全网关，比如公司的防火墙。在这种方式中，当分组通过防火墙时，防火墙封装和解封装分组。通过在安全机器上终止隧道，在公司的LAN上的机器不必懂得IPsec，仅仅防火墙需要懂得IPsec。

34. 网络安全服务的类型有哪些？

解答：网络安全涉及到实体安全和信息的安全。前者主要指计算机网络硬件设备和通信线路的安全性，后者主要包括软件安全和数据安全。ISO 7498-2描述了五种可选的安全服务：身份鉴别、访问控制、数据保密性、数据完整性和不可否认性。与上述五种安全服务相关的安全机制有八种：加密机制、访问控制机制、数字签名机制、数据完整性机制、身份鉴别（认证）机制、通信业务填充机制、路由控制机制、公正机制。此外，还有与系统要求的安全级别直接有关的安全机制，如安全审计、可信功能、安全标记、事件检测和安全恢复等。

35. 可以使用报文摘要（MD）进行数字签名，报文摘要是使用_____的思想对明文进行计算而形成的比特串，发送方是用其__A__ ___B___密钥对报文摘要进行签名。（提示：A在下列1或2中选择正确答案；B在下列3或4中选择正确答案）

（1）公开　（2）秘密　（3）加密　（4）解密

解答：公开密钥算法　A= 2 秘密　B=4解密

36. 试叙述使用公开密钥加密技术的模型描述数字签名的过程。

解答：发送者A使用其私有密钥SKA对报文X进行运算，将结果D_{SKA}（X）传送给接收者B。B使用已知的A的公开加密密钥得出E_{PKA}（D_{SKA}（X））=X。因为除A以外没有别人能具有A的解密密钥SKA，所以除A外没有别人能产生密文D_{SKA}（X）。这样报文X就被签名了。

37. 填空题

使用匿名FTP时，键入_____作为用户标识别，键入____作为口令。

解答：使用匿名FTP时，键入__Anonymous___作为用户标识别，键入__用户邮件地址__作为口令。

38. 试述公开密钥算法的特点和使用公开密钥密码体制的加密/解密过程。

解答：所谓公开密钥密码体制就是使用不同的加密密钥与解密密钥，是一种由已知加密密钥推导出解密密钥在计算上是不可行的密码体制。在公开密钥密码体制中，加密密钥（即公开密钥）是公开的，而解密密钥（即秘密密钥）是需要保密的。加密算法和解密算法也都是公开的。虽然秘密密钥是由公开密钥决定的，但却不能根据公开密钥计算出来。

使用最广泛的MIT的RSA算法有其公开密钥系统的基本特征，包括：

（1）若用公钥对明文加密，再用私钥解密，即可恢复出明文；
（2）加密密钥不能用于解密；
（3）从已知的公钥不能推导出私钥；
（4）使用“已知明文”的攻击方法不能破译出加密的报文；
（5）加密运算和解密运算可以对调。

根据这些特征，在公开密钥系统中，可将公钥PK做成公钥文件发给用户，若用户A要向用户B发送明文M,只需从公钥文件中查到用户B的公钥，设为PKB，然后利用加密算法E对M加密，得密文$C = E_{PKB}(M)$。B收到密文后，利用只有B用户所掌握的解密密钥SKB对密文C解密，可得明文$M = D_{SKB}[E_{PKB}(M)]$。任何第三者即使截获C，由于不知道SKB，也无从解得明文。

39. 什么是量子加密术？

解答：量子加密术的提出主要是为了解决如何在网络上传送只使用一次的密码（one-time pad）的问题。量子加密术是基于这样的事实：光的发射可以取称作光子的分片的形式，它有某种特别的性质，而且光可以通过偏振滤波器而被偏振。如果有一束光（即光子流）通过一个偏振滤波器，从其输出的所有的光子都被偏振在滤波器轴线的方向上。如果该光束通过第二个偏振滤波器，那么输出的光的强度跟两个轴线的夹角的余弦的平方成正比。如果两条轴线互相垂直，那么将没有光子能够通过。

为了产生只使用一次的密码，Alice需要两组偏振滤波器。第一组由一个垂直滤波器和一个水平滤波器构成。这一选择称作直线基准。一个基准就是一个坐标系统。第二组滤波器类似，只是旋转了45度，因此一个滤波器是从左下角到右上角，另一个滤波器是从左上角到右下角。这一选择称作对角线基准。这样Alice有两个基准，她可以随意地插进她的光线。事实上，Alice不必有4个分立的滤波器，而是可以有一个晶体，其偏振可以用电快速交换到4个被允许的方向中的任意一个。Bob具有跟Alice同样的设备。Alice和Bob每一方都具有两个基准对于量子加密术是至关重要的。

现在对于每一个基准，Alice指定一个方向是0，另一个方向是1。假定她选定垂直为0，水平为1。她还选定从左下角到右上角为0，从左上角到右下角为1。她把这些选择用明文发送给Bob。接着Alice基于一个随机数发生器选取一个只使用一次的密码。她把它一位一位地发送给Bob，对于每一位都随机地选取两个基准中的一个发送。每发送一位，她的光子

枪都发射一个适当偏振的光子，使用的是她为那一位选择的基准。例如，她选择的基准序列可以是对角线，直线，直线，对角线，直线等。用这些基准发送只使用一次的密码，她将发送如图9-7（a）所示的光子。给定只使用一次的密码和基准序列，为每一位使用的偏振也就唯一地确定了。

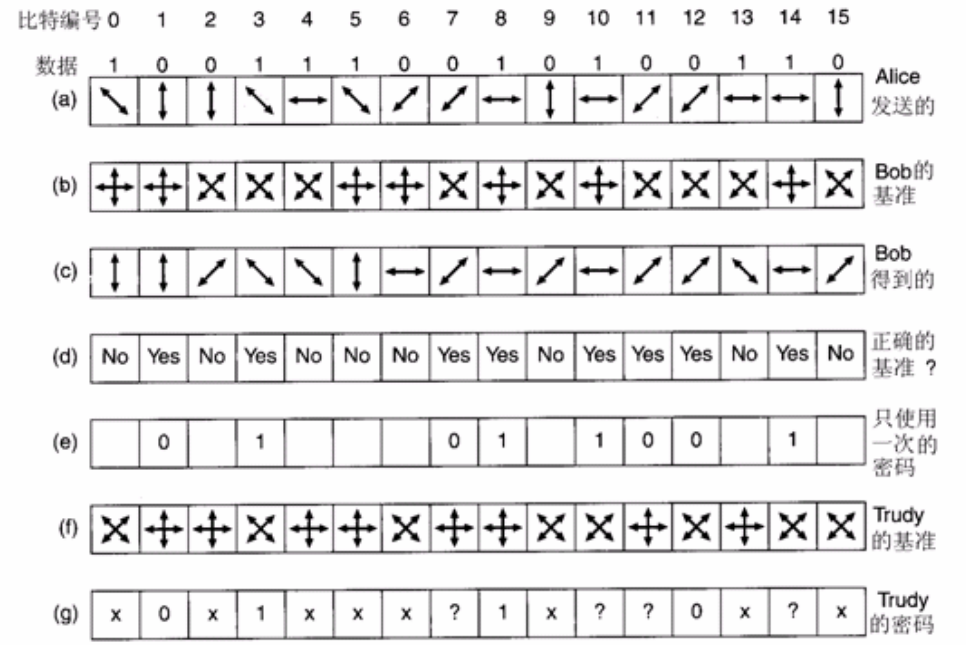


图 9-7　量子密码示例

Bob不知道使用哪个基准，因此他为每个到达的光子随机地选择一个基准，并且就使用它，如图9-7（b）所示。如果他选用了正确的基准，他就得到了正确的比特。如果他选用了不正确的基准，他就得到了一个随机的比特，因为如果一个光子经过的滤波器以相对于它自己的轴线 4 5 度偏振，它就会随机地跳到该滤波器的偏振，或者跳到垂直于滤波器的偏振，而且二者的概率相同。因此，一些位是正确的，一些位是随机的，但Bob不知道哪些对，哪些随机。图9-7（c）示出了Bob得到的结果。

Bob把他为每一位使用的基准用明文告诉Alice，Alice则用明文告诉Bob哪些位的基准是正确的，哪些位的基准是错误的，如图9-7（d）所示。由这些新息他们双方根据正确的猜测可以建立如图9-7（e）所示的位串。平均地讲，这个位串的长度是原始位串长度的一半，但由于双方都知道这一点，他们可以用它作为只使用一次的密码。所有Alice要做的就是发送一个位串，使其长度略大于所需长度的2倍，这样她和Bob就都有了所需要长度的只使用一次的密码。

9.3 综合应用练习题

1．给出两条原因解释为什么PGP要压缩消息？

解答：PGP（Pretty Good Privacy, 相当好的保密性）是一个完整的电子邮件安全包，能够提供加密、鉴别、数字签名和压缩功能，并且都易于使用。发送方先用MD5散列（hash）处理他的消息，然后用他的RSA私钥加密所得到的散列。加密了的散列与原始消息连接在一起产生消息P1，并且用ZIP程序压缩产生P1.Z。下一步，PGP提示发送方输入一个随机数，键入的内容和键入速度被用来生成一个128比特的IDEA消息密钥K_M。IDEA用K_M加密P1.Z。另外，K_M又被用接收方的公钥加密。这两部分被连接在一起，转换成base 64。结果，消息只包含字母、数字、+、/ 和 = 符号。这意味着它可以被放入RFC 822主体内，并且可以不加修改地到达目的地。

压缩的原因，一是可以节省带宽，但更重要地，它也消除了包含在明文中的频度信息（例如，“e”是英语正文中最普遍的字母）。在效果上压缩把明文转变成无意义的字母序列，增加了密码分析员为攻破报文所必须做的工作量。

31．假定Internet上所有的人都使用PGP，那么一则PGP消息能够被发送给任意Internet地址并被所有相关的人正确解码吗？讨论一下你的回答。

解答：不能。假定该地址是一个邮件列表。每个人都会有他自己的公钥，只用一个公钥加密IDEA密钥不管用。它必须用多个公钥加密。

33．PGP（Pretty Good Privacy）不支持规范化，而PEM（Privacy Enhanced Mail）支持，为什么？

解答：对于PGP，身份验证和加密都不是强制性的。如果不进行身份验证，也不加密，那么消息就可以不用base 64编码发送，因此中间节点篡改回车和换行也不是致命的问题。对于PEM，身份验证总是要进行的。因此，当不使用base 64编码时，就必须在应用MD5之前把输入消息转换成标准格式，即规范化。

3. 寻找一个77位的只使用一次的密码，用它从图9-8出的密文产生正文“Donald Duck”。

```
   报文1: 1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
密码1:    1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
   密文: 0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

密码2:    1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
  明文2 : 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011
```

图 9-8　只使用一次的密码的使用示例

解答：要解答本题，首先要懂得什么是只使用一次的密码。该加密方法首先选择一个随机的位串作为密钥。然后把明文转换成一个位串，例如使用它的ASCII表示。最后逐位计算这两个位串的异或运算结果。

“Donald Duck”的ASCII编码是：

1000100　1101111　1101110　1100001　1101100　1100100　0100000　1000100
1110101　1100011　1101011

图9-8中给出的密文是：

0011011　1101011　0011110　0111010　0100100　0000111　0101011　1010011
0111000　0010011　0000101

对上列两个位串做异或操作，运算的结果就是下列要寻找的77位只使用一次的密码：

1011111　0000100　1110000　1011011　1001000　1100010 0001011　0010111
1001101　1110000　1101110。

35．请破译下列单字母表密码。明文仅由字母组成，引自于Lewis Carroll的著名诗句。

```
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
```

解答：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　q　a

根据该单字母表，可得到下列跟本题中给出的单字母表密码对应的明文：

```
the time has come the walrus said to talk of many things
of shoes and ships and sealing wax of cabbages and kings
of 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
```

36．请破译下面的列换位密码。明文取自于一本流行的计算机教材，因此可能会出现“computer”这个词。明文仅由字母组成（无空格）。密文被划分为5个字符的块以方便阅读：

```
a a u a n   c v l r e   r u r n n
d l t m e   a e e p b   y t u s t
i c e a t   n p m e y   i i c g o
g o r c h   s r s o c   n n t i i
i m i h a   o o f p a   g s i v t
t p s i t   l b o l r   o t o e x
```

解答：明文是“a digital computer is a machine that can solve problems for people by carrying out instructions given to it .”

密文6个字母，例如ABCDEF，明文按行书写，从第1列开始按列生成密文如下：

A	B	C	D	E	F
a	d	i	g	i	t
a	l	c	o	m	p
u	t	e	r	i	s
a	m	a	c	h	i
n	e	t	h	a	t
c	a	n	s	o	l
v	e	p	r	o	b
l	e	m	s	f	o
r	p	e	o	p	l
e	b	y	c	a	r
r	y	i	n	g	o
u	t	i	n	s	t
r	u	c	t	i	o
n	s	g	i	v	e
n	t	o	i	t	×

37. 替换和换位可以用简单的电路实现。图9-9（a）所示的设备称为P盒（P是permulation的缩写，中文含义是变序），用以改变8位输入线的输出排列。如果这8位输入从顶至下表示0 1 2 3 4 5 6 7，则该P盒的输出为3 6 0 7 1 2 4 5。通过适当的内部布线，可以让P盒作任意变序，并可以光的速度执行。图9-9（b）所示的S盒实施替换。在示例中，输入3比特的明文，输出3比特的密文。S盒的操作可分为3段：3比特输入选择从第一站伸出的8根线中的一根，并将其置成1，其它线均置成0。第二站是一个P盒。第三站把所选的输入线（置成1的线）按二进制重新编码。在示列中，如果8个八进制数0 1 2 3 4 5 6 7一个接一个地输入，那么输出序列将变为2 4 5 0 6 7 1 3。 这里的P盒也可以通过适当的布线实现任何替换。在具体的实现中，我们可以让P盒和S盒交替出现。虽然这种安排可能符合美学，但如果首先全部是P盒，然后全部是S盒，这样会更安全吗？

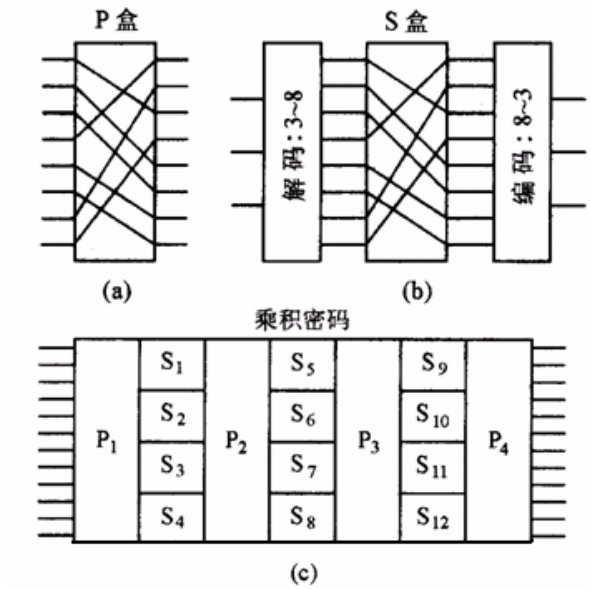


图 9-9　乘积密码的基本元素 （a）P 盒 （b）S 盒 （c）乘积

解答：是的。连续的P盒序列可以用单个P盒替代，连续的S盒序列也类似。

38．假定一则消息用密文块链接方式的DES加密，块C_i中的一比特密文在传输过程中偶然地从0变为1，这将导致多少明文被破坏？

解答：DES相当彻底地混合了一块中的位，因此在块C_i中的单个位错将完全地破坏了明文块P_i。此文在第i+1个明文块P_{i+1}中也将有一位错。然后，所有后随的明文块都将是正确的。因此单个位错仅影响两个明文块。

39．现在再次考虑密文块链接。代替一比特由0变成1，如果把一个额外的0比特插在密文流中块C_i的后面，那么因此将导致多少明文被破坏？

解答：由于插入的0比特将变成块C_{i+1}的第1位，现在从P_{i+1}开始的每一个明文块将都是错误的，因为对异或操作的所有输入（C_{i+1}，C_{i+2}，…）都将是错误的。显然成帧错误要比单个位翻转的错误严重得多。

40．如果明文仅包含大写ASCII字母加上空格、逗号、句号、分号、回车和换行，设计一个破解DES的方法。假定对明文的奇偶检验位一无所知。

解答：使用每个可能的56位密钥来解密第一个密文块。如果结果产生的明文是合法的，再尝试下一块，…等。如果所得的明文是非法的，则再尝试下一个密钥。

41．根据发送一个大文件所需加密操作的次数，比较加密块链接和加密反馈方式，哪一个更高效？高多少？

解答：加密块链接方式每次加密产生8字节输出。加密反馈方式每次加密产生1字节输出。因此，加密块链接方式比加密反馈方式更为高效，前者的效率是后者的8倍，也就是说，在相同数目的周期中，前者可以加密8倍于后者的明文。

4. 量子密码术需要有一个光子枪，它可以按照要求发射单个运载1比特的光子。试计算在一个100-Gbps光纤链路上一个比特运载多少个光子。假定一个光子的长度等于它的波长，并且在本题中它是1微米，光在关纤中的速度是每毫微秒20厘米。

解答：在100Gbps的速度，发送1比特需花时间10^{-11}秒。光在关纤中的速度是每秒2×10^8米.1比特时间所对应的光脉冲传播的长度等于$2 \times 10^8 \times 10^{-11}$米=2000微米。由于一个光子大约1微米长，该脉冲相当于2000个光子长度。因此，即使是100 Gbps的高速度，每比特也不可能接近1个光子。仅当速度达到200Tbps时，我们才能达到每个光子1比特的条件。

5．在使用量子密码术时，如果Trudy捕获并再生了光子，她将使得一些光子变得不正确，所产生的差错会出现在Bob的只使用一次的密码中。平均起来，Bob的只使用一次的密码位有多大比例是错误的？

解答：有一半的时间，Trudy的猜测是正确的。所有那些位都会被正确地再生。另一半时间她的猜测是错误的，给Bob发送随机位。在这些位中，有一半是错误的。因此，在她放到光纤上传输的位中有25%是错误的。总之Bob只使用一次的密码中有75%是正确的，25%是错误的。

6. 基本的密码学原则告诉我们，所有的报文都必须有冗余。但是我们也知道，冗余帮助攻击者分析一个猜测的密钥是否正确。下面考虑两种形式的冗余。第一种，明文的开头n位包含一个已知的图案。第二种，该报文的最后n位包含一个对报文的散列值。从安全的角度看问题，这两种形式对等吗？请讨论你的答案。

解答：如果攻击者有无限的计算能力，二者是相同的，但由于攻击者不可能有无限的计算能力，所以第二种形式较好。它迫使攻击者做一种计算，看尝试的每个密钥是否正确。如果这种计算是代价高的，它将减慢攻击者的速度。

9. 假定1个处理器分析1个密钥花1微微秒的时间，一个具有10^9个处理器的密码攻击机攻破128位版本的AES（高级加密标准）需要10^{10}年。然而，现在的机器可能有1024个处理器，1个处理器分析1个密钥需要花1毫秒的时间。因此，为了达到上述AES攻击机的水平，我们需要在性能上改进一个10^{15}的因子。如果Moore关于每18个月计算能力加倍的定律继续成立，那么即使是建立这样的机器也还要用多少年的时间？

解答：$2^n=15$, $n=15\log_2 10$, $n=50$。

50次加倍共需要1.5年 x 50=75年。因此，即使是建立这样的机器也还要用75年的时间，而且Moore定律从现在开始有可能维持不了75年。

42．对于a=1，b=2，…等，使用RSA公开密钥加密系统

（a）如果p=7，q=11，列出d的5个合法值；
（b）如果p=13，q=31，且d=7，求出e；
（c）p=5，q=11，且d=27，求出e，并加密“abcdefghij”。

解答：（a）p=7，q=11，z=（p-1）×（q-1）=6×10 = 60
因此，d是一个与60互为质数的数，d的5个可能的值是7，11，13，17和19。

（b）p=13，q=31，d=7，z=12×30=360

∵e×d = 1 mod z

∴7e = 1 mod 360

那么7e可能是361，721，1081，1441等。

用7去除这些数中的每一个，看哪一个可以被7整除。结果发现，721÷7=103

∴e=103

（c）p=5，q=11，d=27

z=4×10=40　n=5×11=55　27e = 1 mod 40

27e可能是41，81，121等

∵81可以被27整除，∴ e = 81÷27 = 3

为加密P，我们使用$C = P^3 \bmod n = P^3 \bmod 55$。

对于P=1 到 P=10 （分别对应abcdefghij）求得C分别等于1，8，27，9，15，51，13，17，14和10。

10．AES（高级加密标准）支持256位的密钥。AES-256有多少个密钥？想一想在物理学、化学或天文学中是否遇到过这样大小的数字？这样大的数字说明了什么问题？

解答：2^{256}=10n n=256log2=77

因此，密钥的个数等于10^{77}。

在我们的银河系中的星球个数大约是10^{12}，银河系的个数大约是10^8，因此在宇宙中有大约2^{20}个星球。太阳（典型的星球）的质量是2×10^{23}克，太阳大部分由氢气构成，1克氢气中原子的个数大约是6×10^{23}个。因此在太阳中原子的个数大约是1.2×10^{57}。对于10^{20}个星球，在宇宙中所有星球的原子的数目大约是10^{77}。因此，256位AES密钥的个数等于整个宇宙的数目（忽略黑洞）。由此可以看出，强力攻破AES-256在近期不太可能。

15．假定一个用户Maria发现她的RSA私钥（d1,n1）跟另一个用户Frances的RSA公钥（e2,n2）相同。换句化说，d1=e2,n1=n2。Maria应该考虑改变她的公钥和私钥吗？

解答：Maria应该考虑改变她的公钥和私钥。这是因为Frances相对容易用下述方法计算出Maria的私钥。

Frances知道Maria的公钥（e1,n1），Frances注意到n2=n1，现在Frances可以通过简单地列举方程d1×e1=1modn1的不同的解来猜测Maria的私钥（d1,n1）。

16. 磁盘文件通常是以非连续的顺序访问的，特别是在数据库中的文件。对于一个使用加密块链接方式加密的文件，访问一个随机选择的块需要首先解密在它前面的所有的块，这是一个昂贵的做法。为此，人们提出了如图9-10所示的计数器方式。在这种方式中，明文不是直接加密。取而代之的是，把初始化向量加上一个常数加密，将所产生的密文跟明文异或。通过在每一步对每一个新块都把初始化向量（IV）递增，使得容易解密在文件中任何位置的块而不必首先解密在它前面所有的块。现在考虑计数器方式的使用，并让IV=0。一般说来，0的使用会对密码的安全性有威胁吗？

解答：不会。安全性是基于一个强健的加密算法和一个长的密钥。初始化向量不是影

响安全性的真正重要的因素。密钥是最重要的。

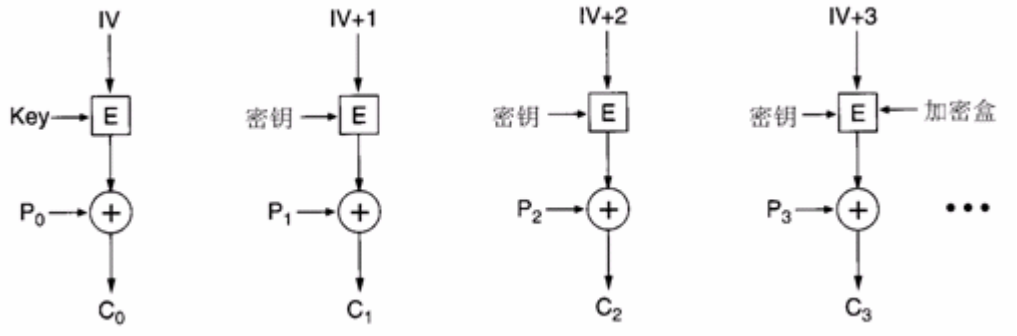


图 9-10　使用计数器方式加密

43．用Diffie-Hellman密钥交换法在Alice 和Bob 之间建立一个秘密密钥。Alice向Bob发送（719，3，191），Bob以（543）回答。Alice的秘密号码x是16，请问密钥是多少？

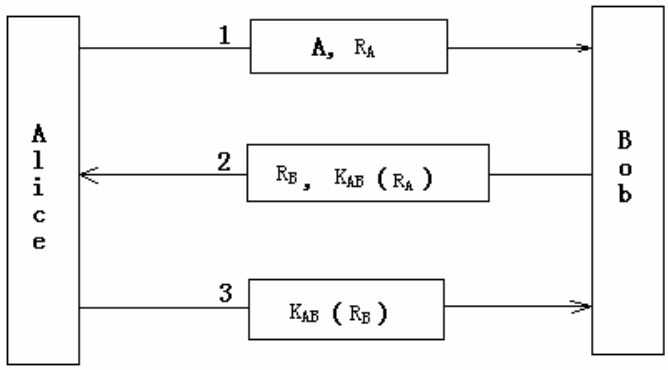
解答：根据Diffie-Hellman算法，为了在Alice 和Bob 之间建立一个秘密密钥，Alice和Bob必须同时知道两个大的质数n和g，并且（n-1）/2 和 （g-1）/2 都是质数。这些质数可以是公开的，因此两人中的任一人都可以选取n和g，并公开地告诉另一方。然后，Alice再挑选一个大数（例如512比特），并将它保密。同样地，Bob选定一个秘密的大数y。Alice首先开始密钥交换协议，她发给Bob一条包括（n，g，g^x mod n）的信息。Bob发给Alice一条g^y mod n的信息作为回答。Alice把Bob发给自己的数字求x次方计算后得到（g^y mod n）^{x}。Bob执行类似的操作得到（g^x mod n）^{y}。根据模的计算原理，两个算式都得到（g^{xy} mod n）。这样Alice和Bob就可以共享一个秘密密钥（g^{xy} mod n）。

现在，n=719，g=3，g^x mod n = 191，g^y mod n = 543，　x=16

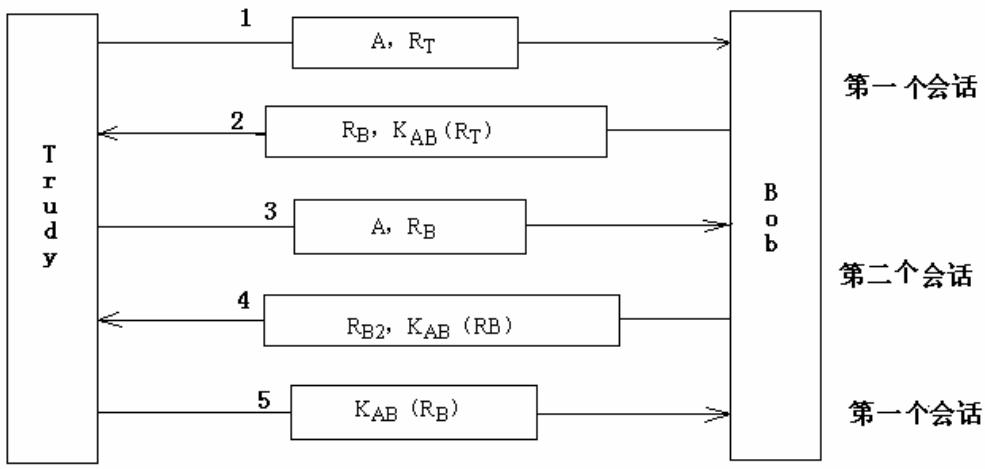
g^{xy} mod n = （g^y mod n）^{x} = 543^{16} mod 719 = 40

所以密钥是40。

44．在缩短的双向鉴别协议中（参见如图9-11a），Alice启动查问-应答协议，发送（A，R_A），Bob在回答Alice查问时也发送自己的查问，发送[R_B，K_{AB}（R_A）]，然后Alice再以[K_{AB}（R_B）]应答。这样整个协议用三次传送完成双向鉴别。但不幸的是，该协议可能被反射攻破。如图9-11（b）所示，Trudy宣称自己是Alice，并发送R_T，Bob像通常那样以自己的查问回答R_B。此时Trudy用第三条信息打开第2个会话，把第2条信息中的R_B作为查问信息。Bob将它加密后，把K_{AB}（R_B）作为第4条信息发回。现在Trudy有了所缺的信息，所以她能够完成第一个会话并放弃第二个。如果我们对协议中的一则信息做小的改动，就能使该协议抵抗反射攻击。请解释需要改动什么。



（a）缩短的双向鉴别协议



（b）Trudy的反射攻击

图 9-11　缩短的双向鉴别协议和 Trudy 的反射攻击

解答：在第2则信息中，把R_B放在加密报文的内部。这样Trudy将不能够找到R_B，因此反射攻击也就不顶用了。

45．在大嘴蛙协议中，为什么A以明文方式发送，并且跟加密了的会话密钥一起发送？

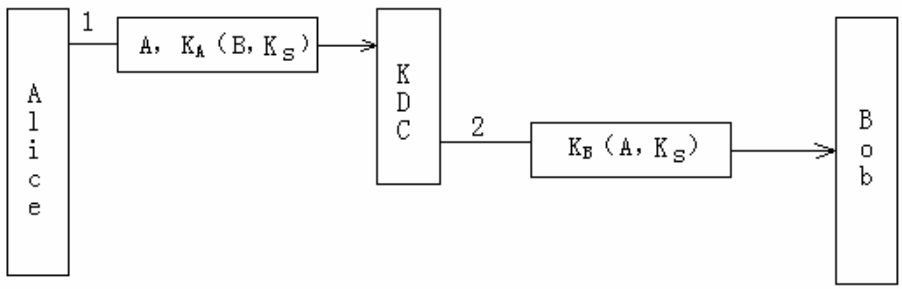


图 9-12　大嘴蛙鉴别协议

解答：在大嘴蛙协议中，每个用户都与密钥分发中心（KDC）共享一个单独的密钥。

鉴别和会话管理都是通过KDC进行的。图9-12示出了典型的大嘴蛙协议交互过程：Alice选择一个会话密钥K_s，然后告诉KDC她想使用K_s与Bob通话。这条消息用Alice与KDC共享的密钥K_A（专用）加密。KDC解密该消息，获得Bob的名字和会话密钥。然后它构成一条包含Alice的名字（图中以A表示）和会话密钥的新消息，并将这条消息发给Bob。这条消息用Bob与KDC共享的密钥K_B（专用）加密。当Bob解密该消息时，他知道Alice想和他交谈，并且知道了她想用的密钥。

在这里，A以明文方式发送，是因为KDC需要某种途径被告知谁发送了该报文，因而才能知道哪一个解密密钥适用于该报文。

46．在大嘴蛙协议中，每则明文消息以32个0开头；这在安全性方面是有风险的。假定每则消息以跟每个用户相关的随机数开始，实际上这相当于仅仅该用户和KDC知道的第二密钥，这样做就可以消除攻破明文的可能了吗？

解答：不可能。攻击者只须捕获来自或前往同一用户的两个报文。然后他可以试用同一密钥破解这两个报文。如果在两个报文中的随机数相同，那么他所使用的密钥就是正确的。实际上，所提出的新机制能够起到的作用只不过是以2倍的因子增加攻击者的工作量。

47．在Needham-Schroeder协议中，Alice产生两条询问，R_A和R_{A2}，这看起来是重复了，能否去掉其中一个？

解答：图9-13示出了一个Needham-Schroeder协议的典型交互过程。协议开始时，Alice告诉KDC她想与Bob通话。该消息包含了一个大随机数R_A作为暂时号。KDC发回第二条消息，包含Alice的随机数，一个会话密钥和一个许可证，Alice可以把这张许可证发给Bob。使用随机数是为了让Alice确信，第二条消息是新的，而不是重发的信息。 Bob的标识名也在其中，这是为了防止攻击者Trudy用他自己的标识名（T）代替第一条消息中的B，从而使得KDC用K_T而不是K_B加密第二条消息末尾的许可证。在加密消息中包含用K_B加密的许可证是为了防止Trudy用其它消息代替它并发给Alice。

Alice将许可证和一个用会话密钥K_s加密的新随机数R_{A2}发给Bob，在第四条消息中，Bob发回$K_s(R_{A2}-1)$以向Alice证明她是在与真正的Bob通话。发回$K_s(R_{A2})$不可行，因为Trudy可能从第三条消息中偷取了它。

收到第四条消息后，Alice确信她正在和Bob通话，因为迄今为止不可能有任何重发消息，她仅在几毫秒前生成R_{A2}。第五条消息的目的是让Bob确信自己正在与Alice通话，同时也没有任何重发消息。由于双方都发了一条查问和做了一个应答，这就排除了任何重发攻击的可能性。

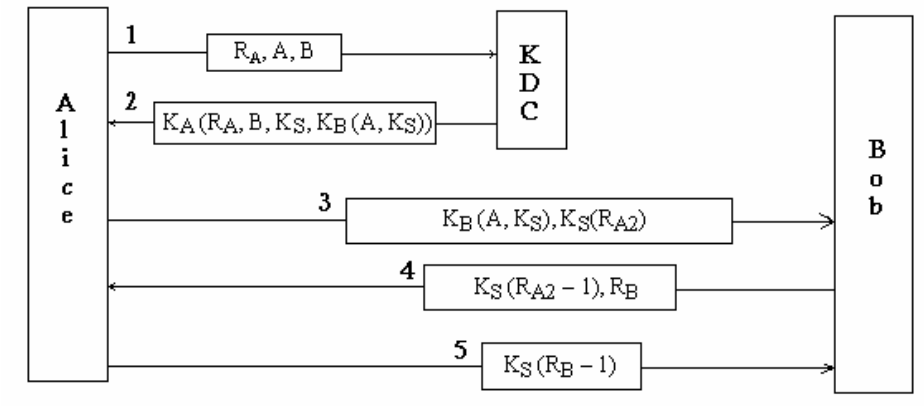


图 9-13　Needham-Schroeder 鉴别协议

随机数R_A和R_{A2}用于不同的目的。使用R_A是要让Alice相信，她是在跟KDC讲话。使用R_{A2}是要让Alice相信，她后来是在跟Bob讲话。这两条询问都是必需的。

18. 图9-14示出，Alice是如何给Bob发送一个签名的报文的。如果Trudy替换P，Bob能够发现。但是如果Trudy同时替换P和签名，会发生什么样的情况？

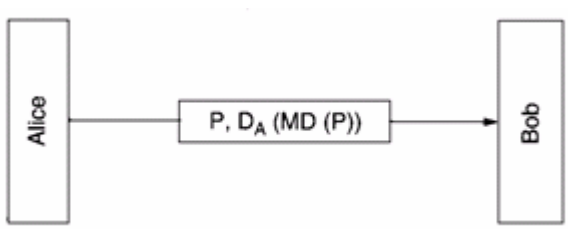


图 9-14　使用报文摘要做数字签名

解答：如果Trudy把两部分都替换，当Bob把Alice的公钥用于签名时，他会得到一些不是明文的报文摘要的内容。Trudy可以放进伪造的报文并对它产生散列值，但她不能够用Alice的私钥对它签名。

19. 数字签名对于懒散用户有一个潜在的缺点。在电子商务活动中，可能要签一个合同，用户被要求用合同内容的散列值签名。如果用户没有实际地验证合同和散列值是互相对应的，用户就可能无意中签署了一个不同的合同。假定Mafia公司尝试利用这个缺点赚钱，他们建立一个收费web站点，并向新客户索取了信用卡号码。然后他们发送过来一个合同，该合同说该客户愿意使用他们的服务，并通过信用卡付费。他们要求客户在合同上签名。他们知道大多数客户只是签名，而不仔细地验证合同与散列值是否一致。试说明Mafia公司如何能够从一个合法的Internet 珠宝商购买金刚石，并且让没有料想到的客户付费。

解答：当一个客户Sam表示要购买某个春画或赌博游戏时，Mafia却用Sam的信用卡从一个珠宝商订购金刚石。但珠宝商发送过来一个待签名的合同（假定该合同包括Sam的信用卡号和作为地址的Mafia邮箱）时，Mafia把珠宝商报文的散列值转发给Sam，同时转发过来的还有要Sam签署的作为春画或赌博游戏的合同。如果Sam盲目地签字而没有注意到合同

和签字的不匹配，Mafia就会把这个签名转发给珠宝商，该珠宝商将把金刚石运送给Mafia。如果Sam后来声明他没有订购金刚石，珠宝商会把一个签了字的合同给他看，表示他订购了。

20．一个数学班有20个学生。至少有两个学生有同样的生日的概率是多少？假定没有人在闰日（2月29日）出生，因此有365个可能的生日。

解答：20个学生，共有20×19÷2=190对。在任意一对中的学生具有相同生日的概率是1/365，他们具有不同生日的概率是364/365。所有190对都具有不同生日的概率是$(364/365)^{190}$，这个数字大约等于0.594，那么有一对或多对具有相同生日的概率就是1－0.594=0.406。

22. 图9－15说明，把用户Bob的公钥放在其网站的网页上不是一个好办法。Trudy可能截取Alice索取Bob公钥的请求而用她的公钥冒充。现在假定Bob和Alice已经共享一个私钥，但是Alice仍然要得到Bob的公约。现在有什么方法可以安全地得到它吗？如果有，是怎么回事？

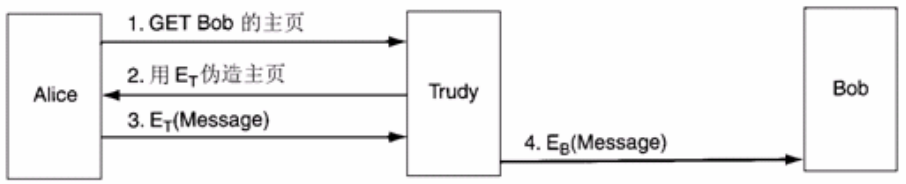


图 9-15　Trudy 破坏公钥加密的方法

解答：这是可以做到的。Alice用共享密钥加密一个词语，把它发送给Bob。Bob用共享私钥发回一个报文，该报文包含所受到的词语、他自己的词语以及公钥。Trudy不能够编造这个报文，如果她发送随机的假词语，当被解密时，它将不会包含Alice的词语。为完善这个协议，Alice用Bob的公钥发回对Bob的词语加密的报文。

48．在图9-16示出的公开密钥签名协议中，在第3条消息中，R_B用K_S加密。这个加密是必需的吗？将它以明文送回可以吗？

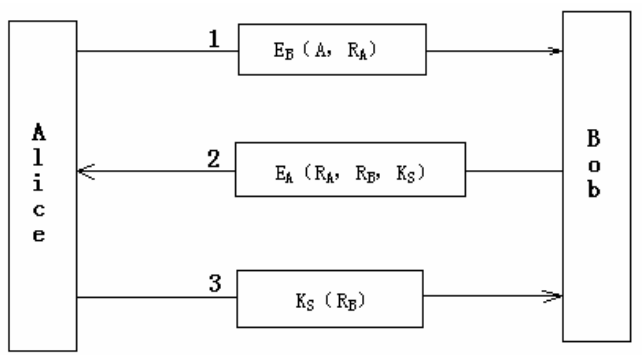


图 9-16　使用公开密钥加密法的相互鉴别

解答：在图9-16中，开始时，Alice用Bob的公开（或加密）密钥E_B加密自己的名字和一个随机数R_A。当Bob收到这条消息后，他并不知道这是来自Alice还是攻击者Trudy，但他仍然发回一条消息给Alice，这条消息包括Alice的R_A，他自己的随机数R_B和一个会话密钥K_S。

Alice收到第二条消息后，她用自己的私有密钥将它解密。她读到了R_A，这让她感觉十分放心。这条消息一定来自Bob，因为Trudy无法得知R_A。另外，由于她刚刚发送R_A给Bob，所以这一定是条新消息，而不是重发消息。Alice发回了第三条消息，表示同意会话。当Bob收到用他刚刚生成的会话密钥加密的R_B后，他知道Alice收到了第二条消息并验证了R_A。

在第3条消息中，对发送的R_B加密不是必需的。攻击者Trudy不知道R_B是否加密，并且R_B将不再被使用，因此它实际上并不是秘密。另一方面，将R_B以密钥K_S加密允许在发送数据之前试用K_S，加倍保证它是正常的。况且，为什么要白白地给予Trudy关于Bob的随机数发生器的信息呢？在一般情况下，还是少以明文方式发送报文为好，再说此处加密操作的开销也不大，所以Alice可能还是要加密R_B。

49．图9-17所示的签名协议有如下缺点：如果Bob崩溃，他可能丢失他的RAM 中的内容。这将导致什么问题？他能做些什么来防止这一情况发生？

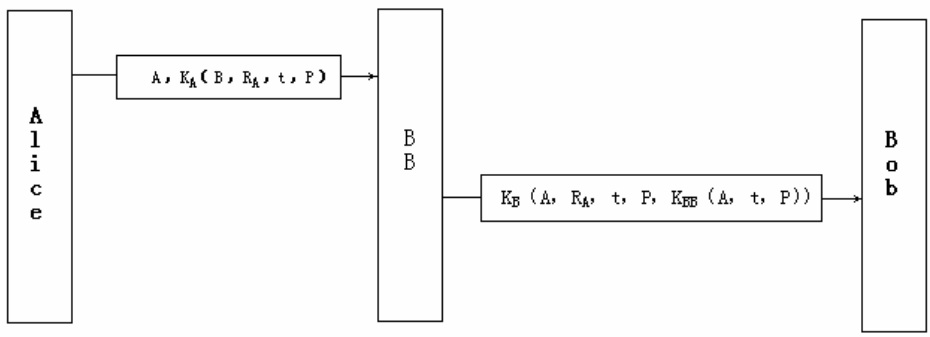


图 9-17　使用 BB 的数字签名

解答：数字签名的一种方法是设立一个众人信任的中央机构，例如名叫BB，每个用户选择一个秘密密钥，并亲手把它交给BB办公室。这样，作为例子，只有Alice和BB知道Alice的密钥是K_A，等等。当Alice想要发送一条签名的明文信息P给她的银行Bob时，如图9-17所示，她生成K_A（B，R_A，t，p）并发送给BB。BB收到这条从Alice来的消息，将它解密，然后交给Bob。发给Bob的消息包括Alice的消息明文和签名信息K_{BB}（A，t，P），其中t是时间戳。Bob现在收到了Alice的请求。

该签名协议有如下缺点：如果Bob崩溃，他可能丢失他的RAM 中的内容。当系统崩溃时，最后一个报文的R_A可能仍然在RAM中。如果这一内容丢失了，攻击者Trudy可能尝试重发最近的报文给Bob，并希望他不会知道这是一个重复报文。

一种解决办法是让Bob在执行每一个请求的操作之前把其入进报文的R_A写到磁盘上。这样就可以使重发攻击者不能奏效。然而，现在又有一个危险，如果在请求被写到磁盘不久就发生崩溃，那么该请求就永远不会被执行了。

50．先阅读下面的一段故事，然后回答问题。

美国一个州立大学的计算机系有一个教员的职位和两个候选人Tom和Dick，Tom比Dick早雇佣两年，因此他优先被考察。如果他被通过了，Dick就没有机会了。Tom知道系主任Marilyn对自己工作评价很高，因此他请求她给院长写封推荐信。Marilyn让她的秘书Ellen给院长写这封信，并简单地叙述了信的内容。Ellen写完信后，。Marilyn检查一遍，计算并签署64比特的摘要，然后Ellen用电子邮件把信发走。对Tom很不幸的是，Ellen正迷恋着Dick，所以想陷害Tom。她以具有32个同义词括号选项的形式写这封信，然后她又写了第二封贬低Tom的信。该信也带有32个同义词括号选项。Ellen让她的计算机整夜地计算每封信的2^{32}个报文摘要。机会在于，第一封信的摘要和第二封信的摘要相同。如果不一样，她可以增加一些选项，在周末再试一遍。假定她找到了一个匹配。我们把赞扬Tom的信叫做A，贬低Tom的信叫做B。Ellen把A信以电子邮件形式发给Marilyn以征求她的同意。Marilyn当然同意，计算出自己的64位报文摘要，签署了该摘要。然而，Ellen把B信寄给院长。收到信和签名的报文摘要，院长对信B运行报文摘要算法，认为确实是Marilyn发送给自己的，就解雇了Tom。

现在的问题是：假定后来Ellen向Marilyn承认了关于在Tom的职位一事上欺骗了她，Marilyn决定以后把信件的内容口述记录到一台录音机上，并让她的新秘书键入。然后Marilyn决定在这些信件被键入以后，在她的终端上检查它们，以确保她的信件正确无误。新的秘书还可以使用类似于Ellen的方法（属于生日攻击方法）篡改信件吗？如果可以，该怎么做？

解答：可以。新秘书可以在信中选取一定数量的空格（比如说，32个空格），可以用空格、退格和空格替换每一个空格。当从终端上观看时，这些替换字符看起来与空格没有什么两样，但它们却产生不同的报文摘要，因此Ellen的生日攻击方法仍然可以起作用。另外，在行的末尾加空格以及交换空格和TAB字符也可以起到类似的作用。

51．使用磁条卡和PIN（个人身份识别号）码的销售点终端有一个致命的缺点：一个坏商人能改变他的磁卡阅读机一捕获和存储磁卡和PIN码上的所有信息，以便以后伪造附加的（假的）交易。下一代的销售点终端将使用带有完整的CPU、键盘和小的显示器的卡。试设计针对这个系统的一个协议，使坏商人无法侵入。

解答：银行给商人的计算机发送一个口令（一个长的随机数），计算机再把口令传给卡。在卡上的CPU以一种复杂的方式变换口令，该方式还依赖于直接输入卡的PIN（个人身份识别号）码。变换的结果被给予商人的计算机传往银行。如果该商人再次呼叫银行运行另一笔交易，银行会发送一个新口令，因此知道老的口令也无济于事。即使该商人知道智能卡的算法，他也不会知道客户的PIN码，因为PIN码是直接输进卡的。在卡上显示的目的是阻止商人显示“购买价是49.95”，而却告诉银行价格是499.95。

23. Alice想使用公约加密法跟Bob通信，她跟Bob建立了一条连接，她希望对方真的就是Bob。她向他请求他的公钥。她把它用明文连同由根CA签发的X.509证书发送给她。Alice执行什么样的步骤验证她是在跟Bob讲话？假定Bob并不介意他在跟谁讲话（比如说，Bob提供一种公用服务）。

解答：第1步使用根CA（证书授权机构）的公钥验证x.509证书。如果证书是真的，她现在就有了Bob的公钥，虽然她应该核对CRL（证书废除列表），如果有一个这样的列表的话。但是，要确定在连接的另一端是否是Bob，她需要知道对方是否有对应的私钥。她挑选一个词语，用Bob的公钥加密发送给对方，如果对方能够把该词语用明文发回，她就相信对方确实就是Bob。

24. 假定一个系统使用基于树形结构体系的CA的PKI（公约基础设施）。Alice想根据Bob通信，并在跟Bob建立一条通信通道后，从Bob收到一个由一个CA　X签发的证书。假定Alice从未听说过X。Alice采取什么步骤验证她是在跟Bob通话？

解答：首先，Alice跟X建立一条通信通道，并请求X验证它的公钥的证书。假定X提供了另一个CA　Y签发的证书。如果Alice不知道Y，她跟Y重复上一步骤。Alice继续做这件事，直到她接受到一个由A签发验证CA　Z的证书，并且Alice知道A的公钥。值得注意的是，这一过程可能继续进行，一直到达根。在此之后，Alice从Z提供的证书开始，以相反的次序验证相关的各个公钥。在验证期间的每一步骤中，她还检查ＣＲＬ（证书废除列表），保证所提供的证书没有被废除。最后，在验证了Bob的公钥之后，Alice使用跟上一习题中相同的方法，确认她是在跟Bob谈话。

25. 如果有一台机器位于NAT（网络地址翻译）设备的后面，能够使用以运输方式运行的具有AH（身份验证头）的IPsec吗？

解答：不能够。运输方式中的ＡＨ在其检验和中包括IP头。NAT设备改变源地址，破坏检验和，所有分组都会被发觉是有错的。

26. 给出ＨＭＡＣ（散列报文鉴别码）对于使用ＲＳＡ签署ＳＨＡ－１散列值的一个优点。

解答：在建立安全关联（SA）的时候，双方协商它们将使用什么样的签名算法。在这里通常不使用公钥加密法，因为必须非常快地处理分组，而所有已知的公钥算法都太慢。由于IPsec是基于对称加密法，发送方和接收方在建立一个SA之前先协商一个共享密钥，将该共享密钥用于签名计算。一个简单的方法是对分组加上该共享密钥计算散列值。当然，共享密钥不被发送。这类机制就被称作ＨＭＡＣ。ＨＭＡＣ对于使用RSA签署SHA-1散列值的一个优点就是ＨＭＡＣ的计算要快得多。

28. 图9-18示出了WEP分组格式。假定检验和是32位，其计算方法是对在载荷中的所有的32位字做异或运算。再假定为了改正RC4存在的问题使用一个没有缺点的流密码，并把初始向量扩展到128位。那么，攻击者是否有办法发现或干扰交通而不会被察觉？

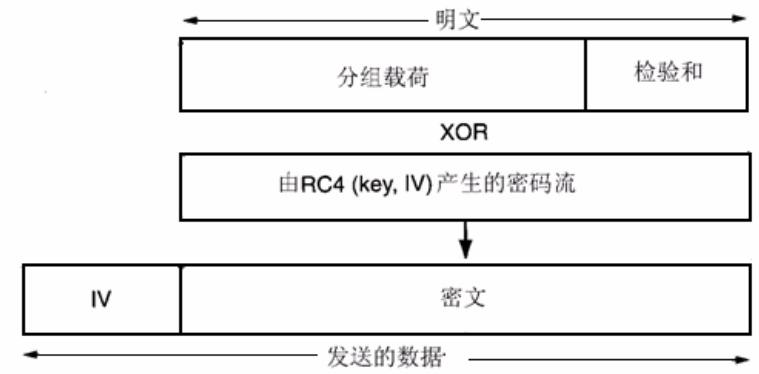


图 9-18　使用 WEP 的分组加密

解答：如图9-18所示，标准的WEP加密使用一个基于RC4算法的流密码。RC4取1-2048位密钥作为种子，把它扩展到一个大得多的长度在内部使用。然后它使用这个内部数字产生一个密码流。在WEP中，通过RC4产生的密码流跟明文异或形成密文。首先，载荷使用CRC-32多项式产生检验和，并把检验和附加到载荷形成准备加密的明文。然后该明文跟一块同样大小的密码流异或。结果就是密文。起始的RC4 的初始向量（IV）被跟密文一起发送。当接收方得到分组时，它从分组中抽出加密载荷，用共享的密钥和刚得到的IV产生密码流，把密码流跟加密载荷异或，即可恢复明文。然后再验证检验和，看报文是否被窜改。

本题中提出了一些改进措施，尽管如此，攻击者还是有办法发现或干扰交通而不被发现的。假定Trudy把一个随机的字跟载荷的开头异或，然后用同样的字跟检验和异或。检验和将仍然是正确的。因此Trudy能够破坏报文并且不被发觉，因为通过加密窜改检验和。

29. 假定一个组织使用VPN通过Internet安全连接它的各个场点，对于一个属于本组织的用户Jim 要跟也属于该组织的另一个用户Mary通信，有必要使用加密或其它的安全机制吗？

解答：如果Jim不想对任何人（即使是他系统的管理员）暴露他跟谁通信，那么Jim需要附加安全机制。记住，VPN仅提供在Internet上（组织外）通信的安全性，它不提供任何在组织内部通信的安全性。如果Jim只想保持他的通信不会受到公司外部的安全威胁，VPN是足够了。

32. 如果Alice和Bob从未见过面，没有共享的密钥，没有证书，不过他们可以使用Diffie-Hellman算法建立一个共享密钥。说明为什么防止中间人的攻击是非常困难的？

解答：凡是Bob知道的，Trudy也可能都知道，任何Bob可以给出的答案，Trudy也可能给出。在这种情况下，Alice不可能知道他是在跟Bob讲话，还是在跟Trudy讲话。

36. 假定一个组织使用Kerberos做身份验证。就安全性和服务可提供性而论，如果AS（身份验证服务器）或TGS（证书授与服务器）崩溃，将会有什么样的影响？

解答：如果AS崩溃，新的合法用户将不能够验证他们的身份，也就是得不到TGS的证书。已经得到一个TGS证书（在AS崩溃之前从AS得到的）的用户可以继续访问服务器，直

到他们的TGS证书（ticket）期满为止。如果TGS崩溃，仅仅已经得到一个服务器s的证书（在TGS崩溃之前从TGS得到的）的那些用户将能够继续访问服务器s，直到他们的服务器证书期满为止。在这两种情况下都不会发生安全违犯的问题。

37．图9-19中示出的攻击者省略了一个步骤。该步骤对于假冒工作不是被需要的，但包括它可能在作案后减少潜在的怀疑。省去的这个步骤是什么？

解答：在步骤3，该ISP请求www.trudy-the-intruder.com，它永远不会被提供。最好提供IP地址，使得改变不显著。结果应该标记成不可缓存，从而使得随后如果需要，还可以再使用这个手段。

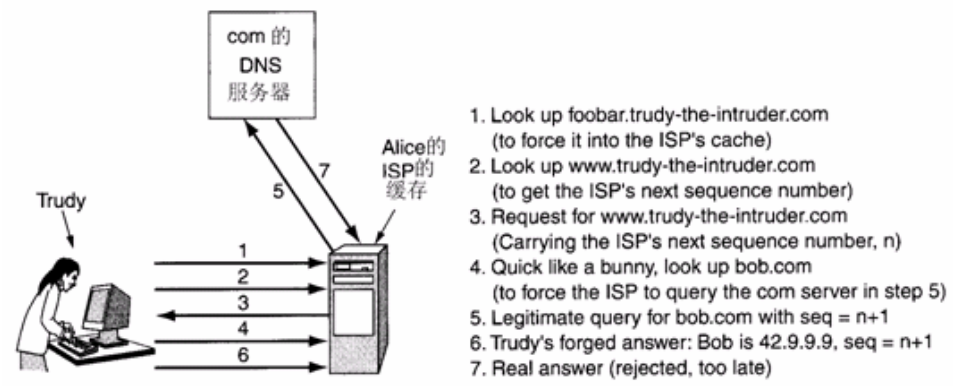


图 9-19　Trudy 如何假冒 Alice 的 ISP

38．有人提出使用ID预估来挫败DNS假冒，让服务器放进一个随机的ID，而不是使用一个计数器。试讨论这一方法的安全性。

解答：DNS代码是公开的，因此用于ID生成的算法是公开的。如果它是一个随机数发生器，使用随机的ID根本不会有什么帮助。使用假冒攻击，Trudy可能知道当前的（随机的）ID。由于随机数发生器完全是确定的，如果Trudy知道一个ID，她可能容易计算下一个。如果由该算法产生的随机数跟时间异或，那会使得它不可预测，除非Trudy也知道时间。把随机数跟时间异或，也跟服务器在最近1分钟内的查询次数（这是Trudy所不致道的），然后取结果的SHA-1散列值，可能会好得多。在这里存在的问题是，SHA-1花了相当长的时间，而DNS必须是快的。

39．SSL（安全套接口层）数据运输协议涉及两个词语，还有一个预主密钥。使用这些词语有什么价值？

解答：这些词语可防止重演攻击。由于每一方都参与密钥的产生，如果一个攻击者尝试重演旧的报文，新产生的密钥将跟旧密钥不匹配。

40．图9-20(b)中的图像包含5个Shakespeare剧本的ASCII正文。是否可以在斑马中间隐藏音乐来取代正文呢？如果可以，它是怎样做到的？在该图画中可以隐藏多长时间的音乐？如果不可以，为什么？

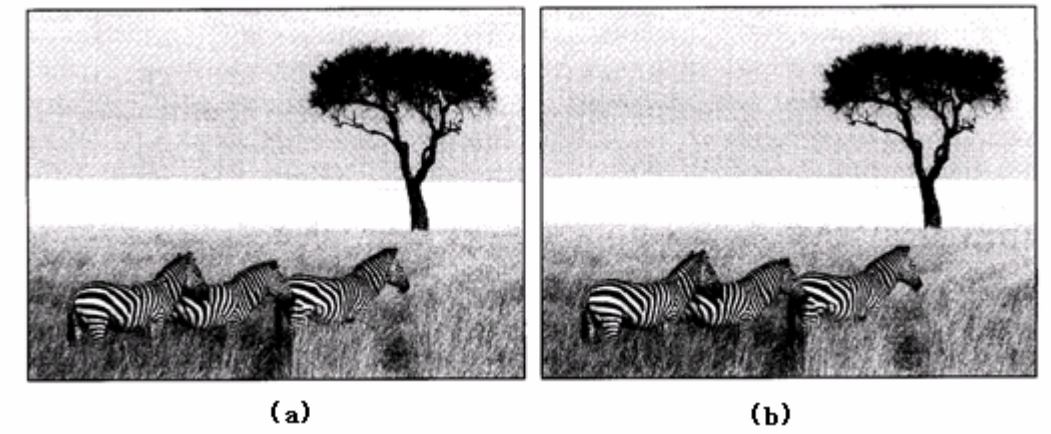


图 9-20 （a）3 个班马和一棵树
（b）3 个班马、一棵树和 5 个 Shakespeare 的完全剧本的正文

解答：图9-20(a)的照片表示3个斑马凝视一棵洋槐树。图图9-20(b)看起来是同样的3个斑马和洋槐树，但它包含Shakespeare的5个完全剧本的正文。原始的彩色图像是1024×768个像素。每个像素由3个8比特数字构成，分别表示那个像素的红、绿、蓝（RGB）的强度。隐藏编码法使用每个RGB颜色的低序位作为隐藏的通道。因此每个像素有3比特用于秘密信息，1比特在红值中， 1 比特在绿值中， 1 比特在蓝值中。在此图像中有1024×768× 3 比特即294,912字节的空间可用于存储秘密信息。用音乐来代替在斑马中间隐藏的正文是容易的，在文件中包含什么样的内容实际上并不影响该方法的有效性。MP3每分钟大约需要 1 MB，294，912÷10^6×60≈18（秒）。因此隐藏大约18秒钟的音乐。

41. Alice是类型 1 匿名再邮器的使用最频繁的用户，她把许多报文投递给自己喜爱的新闻组alt.fanclub.aline，每个人都知道它们来自Alice，因为它们都具有同样的假名。假定再邮器工作正常，Trudy不能假冒Alice。在是类型 1 再邮器都关闭之后，Alice转向一个加密再邮器，并开始了在她的新闻组中的新路线。试设计一种方案，阻止Trudy冒充Alice把新报文投递给该新闻组。

解答：Alice可以散列每个报文，并用她的私钥签署报文。然后，她可以把签署的散列值和她的公钥附加到报文。人们可以比较和验证签名，并把收到的公钥跟Alice上次使用的公钥 比较，如果Trudy尝试冒充Alice和附加Alice的公钥，她不可能得到正确的散列值。如果Trudy使用自己的公钥，人们会看到这跟上次是不一样的，从而使攻击被发现。

42. 在图9-21示出的公钥身份验证协议中，在报文7中的R_B用K_S加密。这个加密是必须的吗？或者说，把它用明文发回就足够了吗？

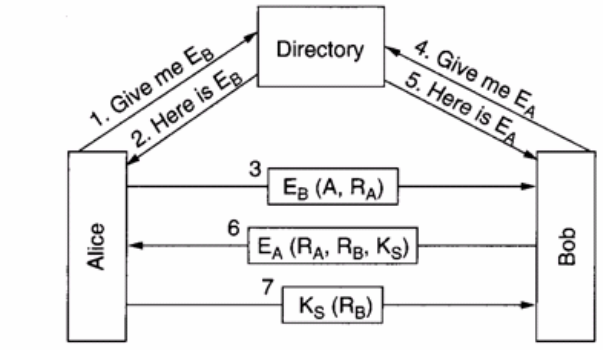


图 9-21　使用公钥加密互相验证

解答：在如图9-21所示的互相验证身份的过程中，开始Alice需要得到Bob的公钥。如果存在一个PKI(公钥基础设施)，有一个目录服务器发放公钥证书，如报文1所示，Alice可以请求Bob的公钥证书。在报文2中的应答是一个包含Bob的公钥的X.509证书。当Alice验证签名是正确时，她给Bob发送一个包含她的ID和一个词语的报文。

当Bob接收到这个报文时，他不知道它是来自Alice还是来自Trudy,但他继续向前进展，向目录服务器请求Alice的公钥（报文4），并且很快就得到了Alice的公钥（报文5）。然后他给Alice发送一个报文（报文6），其中包含Alice的R_A，他自己的词语R_B，以及一个建议的会话密钥K_S。

当Alice得到报文时，她使用自己的私钥将其解密。她看到了其中的R_A，这就给了她一个良好的感觉。报文一定是来自Bob，因为Trudy确定不了R_A，而且它必定是新的，不是重演，因为她只给Bob发送了R_A。Alice通过发回报文7同意会话密钥。当Bob看到用他产生的会话密钥加密的R_B时,他知道Alice得到了报文6，并且验证了R_A。

实际上，给R_B加密不是必须的。Trudy无法知道它，它也不会被再次使用，因此它也并非真正是秘密。在另一方面，这样做允许试用K_S，在发送数据之前双倍保证它管用。而且为什么要给与Trudy关于Bob的随机数发生器的自由信息呢？一般说来，用明文发送的信息越少越好。由于在这里代价很小，所以Alice最好还是加密R_B。

参 考 文 献

1 鲁士文. 现代通信与网络教程. 北京：清华大学出版社，2004

2 谢希仁. 计算机网络. 第4版. 北京：电子工业出版社，2003

3 国务院学位委员会办公室. 同等学力人员申请硕士学位计算机科学与技术学科综合水平全国统一考试大纲及指南. 北京：高等教育出版社，2003

4 鲁士文. 计算机网络—习题与解析. 第1版. 北京：清华大学出版社，2001

5 鲁士文. 计算机网络协议和实现技术. 北京：清华大学出版社，2000

6 Andrew S. Tanenbaum,“Computer Networks”, Fourth Edition, Prentice Hall，2003

7 Ed Tittel. Schaum’s outline of Computer Networking. McGraw-Hill Companies,Inc. 2002

8 Larry L. Peterson & Bruce S. Davie, “Computer Networks: A System Approach.” Second Edition, Morgan Kaufmann Publishers, Inc., 2000

9 Jean Walrand & Pravin Varaiya, “High-performance Communications Networks”, Second Edition, Morgan Kaufmann Publishers, 2000

10 Alberto Leon-Garcia & Indra Widjaja, “Communication Networks:Fundamental Concepts and key Architectures”, McGraw-Hill, 1999